

**CJCSI 3312.01**  
**10 November 2004**

# **JOINT MILITARY INTELLIGENCE REQUIREMENTS CERTIFICATION**



**JOINT STAFF**  
**WASHINGTON, D.C. 20318**

(INTENTIONALLY BLANK)



# CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-2

DISTRIBUTION: A, B, C, J, S

CJCSI 3312.01

10 November 2004

## JOINT MILITARY INTELLIGENCE REQUIREMENTS CERTIFICATION

References: See Enclosure H

1. Purpose. The intelligence certification is a statement of adequacy based on a collaborative, analytical process that evaluates what proposed capabilities will require from or contribute to intelligence enterprise throughout their acquisition lifecycle, and assesses whether the projected intelligence architecture will be available, suitable and sufficient to support those needs. This instruction establishes:

a. Policies, procedures and criteria for the intelligence certification as required by the Joint Capabilities Integration and Development System (JCIDS) in accordance with the CJCS 3170 Series (references a and b).

b. Policies, procedures and criteria for the intelligence review and evaluation of information support plans (ISPs) (formerly command, control, communications, computers and intelligence support plans (C4ISPs)) in accordance with references a, b, d, h and k.

c. Policies and procedures for Defense Intelligence Agency (DIA) validation of threat support to the JCIDS analysis and document development as required by the CJCS 3170 Series (references a and b).

2. Cancellation. None.

3. Applicability

a. This instruction:

(1) Implements the policies and procedures for the intelligence certification process in support of the JCIDS, which replaced the

Requirements Generation System. The procedures and criteria in this instruction will be applied to Initial Capabilities Documents (ICDs), Capability Development Documents (CDDs), Capability Production Documents (CPDs), Capstone Requirements Documents (CRDs) and to Operational Requirements Document (ORDs) updates or annexes (hereafter collectively referred to as "JCIDS documents"). All Joint Requirements Oversight Council (JROC) Interest and Joint Integration program documents will undergo intelligence certification unless a waiver has been granted by J2P-1/ Intelligence Requirements Certification Office (IRCO). Waiver requests will be evaluated on the degree to which a program is determined to consume, produce, process or handle intelligence (throughout any stage of acquisition). Document sponsors should use Enclosure E as the primary guide to assess whether programs produce, consume, process or handle intelligence and should coordinate waiver requests through J2P/IRCO (703-695-4693). All JROC Interest and Joint Integration programs will, at a minimum, undergo DIA threat validation.

(2) Applies to Services, combatant commands, Joint Staff, defense and national intelligence agencies and joint and combined activities.

(3) Also applies to agencies and organizations preparing and submitting ISPs (or legacy C4ISPs) in accordance with references f, h and k. For simplicity and ease of reference, JCIDS documents and ISPs will be collectively referred to in this instruction as "program documents."

b. Documents classified above Secret collateral will also comply with this instruction but may be tailored as necessary to account for special security considerations (see reference b for additional guidance).

c. This instruction does not preclude the need to refer to basic guidance and direction on defense acquisition, the JCIDS or intelligence support to acquisition (references a, b, d, e, f and k).

#### 4. Policy

a. Objectives. Early identification of intelligence support requirements and continuous incorporation of threat intelligence throughout capability development are essential to ensure operational needs of US military forces are satisfied. The objectives of the intelligence certification are to:

(1) Preclude fielding capabilities, systems or programs unsupportable by defense intelligence.

(2) Prevent scientific and technological surprise on the battlefield of the future.

(3) Support national and defense intelligence architecture development through the identification of projected intelligence support shortfalls in order to ensure intelligence support remains effective and responsive to future warfighting needs.

b. Collaboration. In line with the fundamental approach required by the JCIDS, the intelligence certification must be the result of a collaborative process that leverages the unique perspectives of all DOD components' intelligence elements. As illustrated by the collaboration matrix in Enclosure C and the intelligence certification criteria matrix in Enclosure D, there are several key variables in the intelligence certification that rely upon the expertise and unique perspectives within the Service, command or agency intelligence elements. Extensive cooperation, coordination and collaboration are critical to ensure the full range of potential intelligence supportability issues is addressed.

c. Intelligence Certification

(1) The intelligence certification will evaluate program documents' intelligence support needs for completeness, supportability and impact on joint intelligence strategy, policy and architectural planning. The certification will also evaluate intelligence-related systems with respect to security and intelligence interoperability standards. The J-6 interoperability certification is conducted in a separate, but related process, documented in reference d. The specific procedures, criteria and intelligence support definitions used during the intelligence certification are covered in Enclosures B, D, E and G, but descriptions of these certification categories are provided below:

(a) Completeness. Completeness refers to the extent to which a document addresses requirements *for* intelligence support and program compliance with requirements *by* intelligence as examined below.

1. Requirements *for* intelligence support. Although the ability to identify and refine intelligence support needs increases as a capability becomes more defined within the JCIDS process, program documents must, as specifically as possible, declare requirements for intelligence support throughout the program's expected life cycle. This includes projected requirements for all intelligence information (e.g., analytical products), infrastructure (e.g., intelligence systems, processes) or resources (e.g., intelligence funding, personnel) and must include required qualitative and quantitative attributes (see reference b). Enclosure E provides general descriptions of intelligence support

categories (as listed in Enclosure D), associated qualitative and quantitative attributes and associated capabilities. Enclosure G provides guidance on incorporating intelligence support information in specific paragraphs of JCIDS documents.

2. Requirements *by* Intelligence. Documents must also address compliance with requirements imposed *by* intelligence, such as security considerations, classification levels for required information and systems, releasability and interoperability with supporting intelligence systems. Enclosure D provides additional guidance on these certification criteria.

(b) Supportability. Supportability refers to the availability, suitability and sufficiency of the required intelligence support. Assessing supportability requires the comparison of a document's stated or derived intelligence support needs with the expected intelligence capabilities as projected throughout a program's life cycle. The ability to adequately assess supportability depends upon the completeness of support requirement declaration, and must also be evaluated within the context of any shortfall mitigation strategies identified. Although availability, suitability and sufficiency are outlined separately below, these criteria often blend together and do not necessarily represent discrete assessments.

1. Availability: whether the intelligence information, infrastructure or resources are, or are expected to be, available (i.e., in existence) to support the operational capability throughout all phases of its life cycle.

2. Suitability: whether the intelligence information, infrastructure, or resources are, or are expected to be, suitable or appropriate to support the operational capability.

3. Sufficiency: whether the intelligence information, infrastructure or resources are, or are expected to be, sufficient or adequate to support the operational system or program. Sufficiency may apply to both quantitative as well as qualitative aspects of intelligence support.

(c) Impact on Intelligence Strategy, Policy and Architecture Planning. Impact, within this context, refers to the identification of additional inputs to or outputs from the intelligence infrastructure. Requirements for intelligence support may be transparent with regard to the intelligence support infrastructure if planned products, information or services are already projected to be available, suitable and sufficient throughout a program's life cycle. In other cases, programs may require

new types of support altogether or have increased standards for existing support. These additional inputs or outputs may require changes across the doctrine, organization, training, materiel, leadership & education, personnel and facilities (DOTMLPF) spectrum; these potential changes constitute impact on intelligence strategy, policy and architecture planning. The impact assessment provides a mechanism for providing critical feedback to the defense and national intelligence communities to highlight potential shortfalls in current or planned intelligence support.

d. Threat Validation. Acquisition systems or capabilities expected to operate in a threat environment (lethal or non-lethal) shall be based on validated threat information appropriate to the proposed system or capability throughout its projected lifespan. Acquisition systems or capabilities shall also, throughout their lifespan, account for threats to research, development, test and evaluation and production and maintenance, based upon validated threats from technology transfer, espionage and other adversarial collection efforts.

(1) Early and continued collaboration among the intelligence, counterintelligence, capability development and acquisition management communities shall be maintained throughout the JCIDS process to help maintain and ensure technological superiority over adversarial capabilities. This shall begin with the anticipated range of broad capabilities that adversaries might employ as inputs to the Functional Area Analysis (FAA) (reference b). Operational tasks, conditions and standards identified in the FAA should then be submitted to DIA to enable production of an Initial Threat Warning Assessment (ITWA). The ITWA will identify projected adversarial threat capabilities, to include scientific and technological developments that could specifically affect program design or implementation. In addition, DIA will help the sponsor ensure accurate and timely incorporation of adversarial capabilities throughout the remainder of the program's JCIDS process; this can include the provision of an intelligence liaison officer to support the program.

(2) For all JCIDS documents designated JROC Interest or Joint Integration, DIA will validate threat support integration into JCIDS analysis and document development by evaluating respective document threat sections for appropriateness of judgments, consistency with DIA- or Service-validated assessments, currency of documents referenced and the logic of extrapolations derived from existing intelligence. Criteria for the threat validation can be found in Enclosure D.

5. Definitions. Definitions are provided in the Glossary (Enclosure GL).

6. Responsibilities. Responsibilities are provided in Enclosure A.

7. Summary of Changes. This CJCSI replaces and supersedes the 21 February 1997 draft of Joint Military Intelligence Requirements Certification Concept of Operations (CONOPS).

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other federal agencies and the public may obtain copies of this instruction through the unclassified Internet from the CJCS Directives Home Page -- [http://www.dtic.mil/cjcs\\_directives](http://www.dtic.mil/cjcs_directives), as well as on the Secret Internet Protocol Router Network (SIPRNET) at <http://www.dia.smil.mil/intel/j2/j2p/irco/main.html>, and the Joint Worldwide Intelligence Communication System (JWICS) at [http://j2irco.dia.ic.gov/pls/irco/open\\_docs](http://j2irco.dia.ic.gov/pls/irco/open_docs) (under "Certification Process"). Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

9. Effective Date. This instruction is effective upon receipt.



NORTON A. SCHWARTZ  
Lieutenant General, USAF  
Director, Joint Staff

Enclosures:

- A--Responsibilities
- B--Intelligence Certification Procedures
- C--Intelligence Certification Collaboration Matrix
- D--Intelligence Certification Criteria
- E--Intelligence Support Requirement Category Descriptions
- F--Intelligence Certification Summary and Letter
- G--Program Document Guidance
- H--References
- GL--Glossary



DISTRIBUTION

Distribution A, B, C and J plus the following:

	<u>Copies</u>
Secretary of Defense .....	2
USD(AT&L) .....	2
USD(I) .....	2
USDP .....	2
ASD(NII)/DOD CIO .....	2
DOT&E .....	2
D, PA&E .....	2
Director of Central Intelligence .....	2

(INTENTIONALLY BLANK)

## LIST OF EFFECTIVE PAGES

The following is a list of effective pages for CJCSI 3312.01. Use this list to verify the currency and completeness of the document. An “O” indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
1 thru 6	O	E-1 thru E-12	O
i thru viii	O	F-1 thru F-2	O
A-1 thru A-6	O	G-1 thru G-12	O
B-1 thru B-8	O	H-1 thru H-2	O
C-1 thru C-2		GL-1 thru GL-9	
D-1 thru D-9			

(INTENTIONALLY BLANK)

## RECORD OF CHANGES

[illegible]

(INTENTIONALLY BLANK)

## TABLE OF CONTENTS

	Page
Cover Page .....	1
Distribution.....	i
List of Effective Pages .....	iii
Record of Changes.....	v
Table of Contents .....	vii

### ENCLOSURES

#### A – RESPONSIBILITIES

Joint Staff, J-2.....	A-1
Joint Staff, J-6.....	A-2
Joint Staff, J-8.....	A-2
Director, Defense Intelligence Agency .....	A-2
Director, National Geospatial-Intelligence Agency.....	A-3
Director, National Security Agency/Central Security Service .....	A-3
Director, National Reconnaissance Office .....	A-4
Military Services .....	A-4
Combatant Commanders .....	A-5
Defense Information Systems Agency/Joint Interoperability Test Command .....	A-5

#### B – INTELLIGENCE CERTIFICATION PROCEDURES

Purpose .....	B-1
General.....	B-1
Certification Process .....	B-2
Intelligence Certification .....	B-5
Certification Failure .....	B-8

#### C – INTELLIGENCE CERTIFICATION COLLABORATION MATRIX

#### D – INTELLIGENCE CERTIFICATION CRITERIA

#### E – INTELLIGENCE SUPPORT REQUIREMENT CATEGORY DESCRIPTIONS

Intelligence Manpower .....	E-1
Intelligence Resource Support.....	E-1
Collection Management Support .....	E-2
Signature Support/Denial and Deception Analytical Support.....	E-3

Geospatial Intelligence and Services Support .....	E-3
Targeting Support.....	E-4
Combat Search and Rescue Intelligence Support.....	E-6
Joint Intelligence Preparation of the Battlespace/Intelligence Preparation of the Battlespace .....	E-6
Warning Support .....	E-8
Space Intelligence Support.....	E-9
Counterintelligence Support .....	E-9
Intelligence Training Requirements .....	E-10
Dissemination Support .....	E-10

## F – INTELLIGENCE CERTIFICATION SUMMARY AND LETTER

Intelligence Certification Summary .....	F-1
Example of Intelligence Certification Letter .....	F-2

## G – PROGRAM DOCUMENT GUIDANCE

Purpose .....	G-1
General .....	G-1
Leverage the ISP Process .....	G-1
Joint Capabilities Integration and Development System Document Development.....	G-1
Developing Paragraph 9 of Capability Development Documents/ Capability Production Documents Intelligence Supportability ....	G-8
Information Support Plan Document Development.....	G-10

## H – REFERENCES

GLOSSARY.....	GL-1
---------------	------

## TABLES AND FIGURES

Figure B-1. JCIDS and ISP Process Linkage .....	B-2
Figure B-2. Final Intelligence Certification Process.....	B-5
Figure B-3. Intelligence Supportability Risk Scale .....	B-7
Table D-1. Threat Validation .....	D-2
Table D-2. Intelligence Support Criteria .....	D-3
Table D-3. Interoperability Criteria.....	D-7
Table D-4. Security Criteria .....	D-8
Table D-5. Consistency with Joint Intelligence Policy, Strategy, Doctrine, Guidance and Architecture and Planning.....	D-9
Table G-1. ICD Intelligence Considerations .....	G-3
Table G-2. CDD and CPD Intelligence Consideration.....	G-4
Table G-3. ORD/ORD Annex/ORD Update Considerations .....	G-6
Table G-4. ISP Intelligence Considerations .....	G-11



ENCLOSURE A  
RESPONSIBILITIES

1. Joint Staff, J-2:

a. Provide intelligence support and advise the Joint Requirements Oversight Council (JROC) (and supporting organizations) on intelligence supportability and intelligence interoperability issues in support of the JCIDS as required by references a, b and bb.

b. As the certifying official on behalf of the JROC, implement the procedures of this CJCSI. The Intelligence Requirements Certification Office (IRCO) (J2P-1/IRCO) will facilitate the certification process outlined in Enclosure B on behalf of the J-2. In order to provide a comprehensive, robust intelligence certification, J2P-1/IRCO will receive, integrate and consolidate DOD-wide intelligence review comments and recommendations from the Military Services, combatant commands, the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Security Agency/Central Security Service (NSA/CSS), the National Reconnaissance Office (NRO) and other Defense agencies as appropriate.

c. Review all JCIDS program documents, regardless of Acquisition Category (ACAT) level, for intelligence relevance.

d. Conduct an intelligence certification of program documents for those proposed programs that consume, produce and/or process or handle intelligence information in accordance with references a, b and h.

e. Provide intelligence certification to the lead Functional Capability Board (FCB) for JROC Interest designated programs or to the sponsoring DOD component or agency for Joint Integration designated programs.

f. As needed, establish and chair Intelligence Certification Working Groups (ICWGs) to review and resolve issues relating to intelligence certifications. ICWGs may include representatives of the Joint Staff (J-2/J-3/J-6/J-8), Services, defense and national intelligence agencies, and combatant commands as necessary to resolve issues of concern.

g. Coordinate with other joint staff elements, Defense Information Systems Agency (DISA), the Office of the Undersecretary of Defense for Intelligence (USD(I)), the Office of the Assistant Secretary of Defense (Networks and Information Integration) (ASD(NII)) and members of the

Intelligence Community (IC) regarding intelligence-related interoperability concerns and issues.

h. Provide the Battlespace Awareness Functional Capability Board (BA FCB) and associated Working Group (BAWG) with an Intelligence Certification Summary (see Enclosure F) to assist the BA FCB in their responsibilities to identify, analyze, prioritize and validate joint warfighting capability needs in the area of intelligence. Brief the BAWG and BA FCB as required on intelligence issues identified through the certification process. J2P-1/IRCO will provide Intelligence Certification Summaries to other FCBs upon request.

i. Recommend policy and guidance to the JROC concerning the intelligence requirements certification process and intelligence supportability issues, as appropriate.

2. Joint Staff, J-6:

a. Provide command, control, communications and computers (C4) expertise to J-2 during certification of intelligence-related information system interoperability requirements.

b. Participate in ICWGs, as requested, to provide advice on C4 requirements and the C4 concerns of the combatant commands and the Services.

3. Joint Staff, J-8: participate in ICWGs, as requested, to provide advice and expertise on the JCIDS process, as well as operational requirements and concerns of the combatant commands and Services (in the absence of those organizations).

4. Director, Defense Intelligence Agency (DIA):

a. Provide intelligence support and advise the JROC (and supporting organizations) on adversarial capabilities in support of the JCIDS as required by reference i.

b. Validate threat information used during JCIDS analysis, document development or projected threat information needs for future development or testing in accordance with references a and b.

c. As the DOD Functional Managers of both defense Human Intelligence (HUMINT) and Measurement and Signatures Intelligence (MASINT) in accordance with references z and i respectively, DIA will assess defense HUMINT, MASINT, all-source collection management and counterintelligence support requirements for completeness,

supportability and impact on associated strategy, policy and architecture planning. DIA will also evaluate open systems architectures, interoperability and security standards for defense HUMINT and MASINT-related intelligence systems. DIA will additionally participate in ICWGs as appropriate.

d. The National Signatures Program Systems Management Office (NSP/SMO) resident in DIA/DT will assess and evaluate the ability of the National Signatures Community to support signature requirements of or for associated sensing capabilities.

5. Director, National Geospatial-Intelligence Agency (NGA), as the DOD functional manager for imagery, imagery intelligence (IMINT) and geospatial investment activities in accordance with references x and y, will:

a. Designate a point of contact (POC) to serve as a focal point for the coordination and collaboration required by the intelligence certification of program documents.

b. Assess intelligence support requirements for completeness, supportability and impact on geospatial intelligence strategy, policy and architecture planning. NGA will also evaluate open systems architectures, interoperability and compatibility standards for geospatial intelligence-related information systems. NGA will provide J2P-1/IRCO with comments and recommendations for DOD-wide collaboration in accordance with Enclosures B and G, with specific regard to NGA-unique contributions as identified in Enclosure D.

c. Participate in ICWGs, as requested to provide advice and expertise on geospatial intelligence support to the operational requirements in program documents.

6. Director, National Security Agency/Central Security Service (NSA/CSS), as the DOD Functional Manager for Cryptology in accordance with reference aa, will:

a. Designate a POC to serve as a focal point for the coordination and collaboration required by intelligence certification of program documents.

b. Review the intelligence support and intelligence-related operational requirements specified in or derived from program documents. Provide J2P-1/IRCO with comments and recommendations (in accordance with Enclosures B and G) with specific regard to the NSA/CSS-unique concerns as identified in Enclosure D. When applicable, provide feedback on projected impact to cryptologic (signals intelligence [SIGINT])

and information assurance [IA]) strategy, policy and architecture planning. Evaluate open systems architectures, interoperability and compatibility standards for cryptologic and cryptologic support systems to include multi-INT cross-cueing capabilities.

c. In conjunction with similar responsibilities defined in reference d, provide expertise and assistance in assessing that there will be an adequate level of IA to meet the information threat identified.

d. Participate in ICWGs, as requested to provide advice and expertise on cryptologic support (which includes SIGINT) to the operational requirements in program documents.

7. Director, National Reconnaissance Office (NRO):

a. Designate a POC to serve as a focal point for the coordination and collaboration required by intelligence certification of program documents.

b. Review the intelligence support and intelligence-related operational requirements specified in or derived from program documents and provide J2P-1/IRCO with comments and recommendations (in accordance with Enclosures B, D and G). If applicable, provide feedback on projected impact to space intelligence, space control and access, SIGINT, IMINT, MASINT, combat search and rescue (CSAR) or personnel recovery, indications and warning and satellite communications support strategy, policy and architecture planning.

c. In conjunction with similar responsibilities defined in reference d, provide expertise and assistance in assessing that there will be an adequate level of IA to meet the information threat identified.

d. Participate in ICWGs, as requested to provide advice and expertise on areas identified in paragraph 8b above with respect to support to the operational requirements in program documents.

8. Military Services. Each Service will:

a. Designate a POC to serve as a focal point for the coordination and collaboration required by the intelligence certification of program documents.

b. Review the intelligence support and intelligence-related operational requirements specified in (or derived from) program documents. Provide J2P-1/IRCO with comments and recommendations (in accordance with Enclosures B and G) related to the completeness, supportability and

impact of intelligence support requirements, with specific regard to Service unique contributions as identified in Enclosure D.

c. Participate in ICWGs, as requested, to provide advice and expertise on the intelligence-related operational requirements of concern to the Service.

9. Combatant Commanders. The combatant commanders will review and comment on all JROC Interest documents as part of the routine JCIDS staffing process (reference a). Combatant commanders also are provided the opportunity to review and comment on Joint Integration documents during the J-2 and J-6 certification processes. Combatant commanders are invited to review ISPs for acquisition programs at all ACAT levels. In conjunction with these procedures and to help facilitate the DOD-wide collaboration required by intelligence certification of JCIDS documents, combatant commanders will:

a. Designate a POC to serve as a focal point for the coordination and collaboration required by the intelligence certification of program documents.

b. Review the intelligence support and intelligence-related operational requirements specified in or derived from program documents. Provide J2P-1/IRCO with comments and recommendations (in accordance with Enclosures B, D and G) with regard to the unique perspective of the respective command.

c. Participate in ICWGs, as requested, to provide advice and expertise on the intelligence-related operational requirements of concern to the command.

10. Defense Information Systems Agency/Joint Interoperability Test Command (DISA/JITC). JITC conducts interoperability certification testing and assessments of all Information Technology (IT) and National Security Systems (NSS), including intelligence information systems (see references d and h for more information). In this capacity, JITC will:

a. Designate a POC to serve as a focal point for the coordination and collaboration required by the intelligence certification of program documents.

b. As appropriate, provide interoperability expertise to J2P-1/IRCO during certification of intelligence-related information systems or certification of other capabilities supported by intelligence information systems.

- c. Participate in ICWGs, as requested, to provide advice on interoperability considerations related to intelligence information systems or other capabilities supported by intelligence information systems.

ENCLOSURE B

INTELLIGENCE CERTIFICATION PROCEDURES

1. Purpose. This enclosure describes the procedures used during the Intelligence Certification process. This process will help identify potential intelligence shortfalls and make recommendations to the defense and intelligence communities regarding the availability, suitability and sufficiency of future intelligence capabilities. The goal of this process is to preclude acquisition of unsupportable systems as well as to keep development of intelligence capabilities focused on the future needs of the warfighter and appraised of current and projected threat capabilities.

2. General

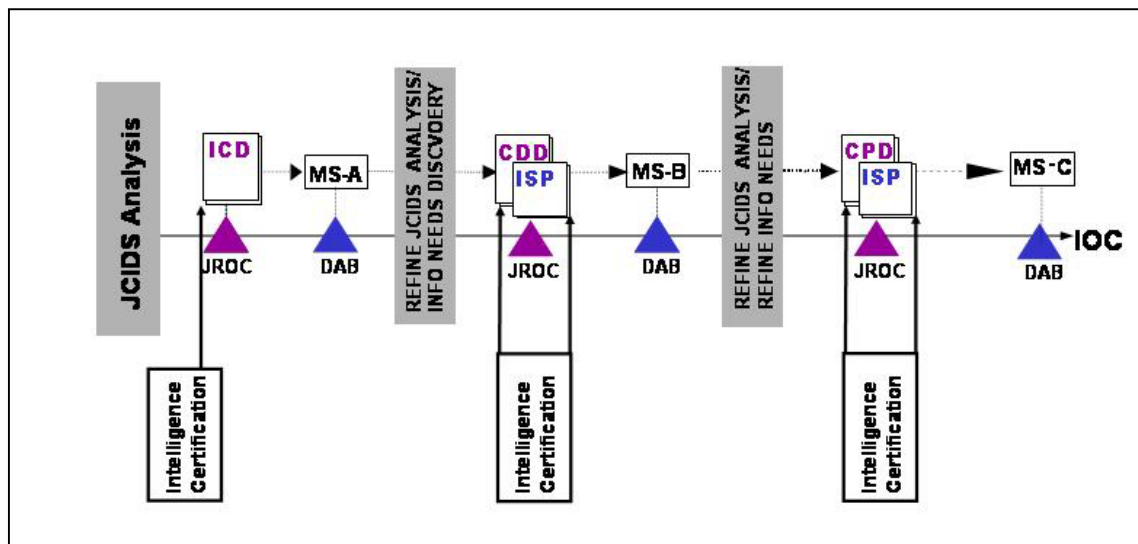
a. The intelligence certification process for JCIDS documents begins when a DOD component submits a draft document to the Knowledge Management/Decision Support (KM/DS) tool for Joint Potential Designator (JPD) assignment through the Gatekeeper process as outlined in references a and b. Following JPD assignment, the document will move into the JCIDS staffing and approval process as outlined in reference b. Unless a waiver has been granted by J2P-1/IRCO, an intelligence certification will be conducted for all JROC Interest or Joint Integration programs. All JROC Interest and Joint Integration program documents will, at a minimum, undergo DIA threat validation. The intelligence certification process for a specific document ends upon completion of Flag-review comment resolution; intelligence certification failure is detailed in paragraph 5 below.

b. ASD(NII) will initiate the staffing of ACAT I and Office of the Secretary of Defense (OSD)-designated special interest ISPs through the Joint C4I Program Assessment Tool-Empowered (JCPAT-E) in accordance with reference h. This tasking will include a requirement for the intelligence certification.

c. To ensure document dissemination for intelligence reviewers without access to KM/DS or JCPAT-E (hosted on the SIPRNET), J2P-1/IRCO) will post documents undergoing intelligence certification on the IRCO's Web portal (on the Joint Worldwide Intelligence Communications System [JWICS]) at: [http://j2irco.dia.ic.gov/pls/irco/open\\_docs](http://j2irco.dia.ic.gov/pls/irco/open_docs).

### 3. Certification Process

a. Staffing and Coordination. The intelligence certification will be the result of two comprehensive, collaborative and iterative reviews that correspond with the associated O-6 and Flag reviews and includes the subsequent Flag-comment resolution phases of program documents. The intelligence certification process will leverage off existing staffing processes IAW references b and d, although J2P-1/IRCO will facilitate internal tasking of documents to DIA and J-2 elements. As documents proceed through staffing, the J-2P/IRCO will conduct and coordinate collaborative reviews for completeness, intelligence supportability and impact as defined by this instruction. Intelligence certification will be tied to a specific document and its associated specific acquisition milestone (e.g., the Milestone B CDD for the first increment of a program). Figure B-1 depicts the intelligence certification and its linkage to the JCIDS and ISP processes.



See Glossary for acronyms.

Figure B-1. JCIDS and ISP Process Linkage

In conducting these reviews, J-2 relies on the insights and expertise provided by reviewers throughout the defense and intelligence communities. These groups provide an early, balanced and robust assessment of the completeness and supportability of intelligence support requirements as projected in program documents and their associated projected impact to the Battlespace Awareness Joint Functional Concept and joint integrated architecture.



b. Intelligence Certification Stages. The intelligence certification process includes three distinct stages.

(1) O-6 /Stage I Reviews. The first iteration of inputs to the intelligence certification process corresponds with the associated O-6 review for JROC Interest (IAW reference b) or Stage I review of Joint Integration documents and ISPs (IAW references b and d).

(2) Flag/Stage II Reviews. The second iteration of inputs to the intelligence certification process corresponds with the associated O-7/Flag review for JROC Interest (IAW reference b) or Stage II review of Joint Integration documents and ISPs (IAW references b and d).

(3) O-7 Comment Resolution/Stage III. The third stage of the intelligence certification process corresponds with:

(a) the comment resolution period following the O-7/Stage II reviews,

(b) the subsequent posting of the document's FCB draft and O-7/Stage II comment resolution matrix to the appropriate staffing tool (KM/DS or JCPAT-E, respectively) and

(c) the receipt and evaluation of collaborative reviewer comments. Comments that are not directly related to criteria in this instruction will not be considered in the certification decision. If all intelligence certification requirements have been met, the VJ-2 will issue an intelligence certification letter (as depicted in Enclosure F) for JROC Interest programs. For Joint Integration programs, the J2P will provide an intelligence certification letter on behalf of the VJ-2 to the lead FCB. Certification letters will be posted to the appropriate staffing tool (KM/DS or JCPAT-E). Intelligence certification failure is addressed in paragraph 5 below.

c. Collaborative Inputs. To ensure the intelligence certification process leverages the unique intelligence perspectives of all DOD components, J2P-1/IRCO will receive inputs from:

(1) Directed reviews by subject matter experts within DIA and J-2, using Enclosure C as a guide for staffing.

(2) Comments and recommendations provided to J2P-1/IRCO by intelligence reviewers from the commands, Services, NGA, NSA/CSS, NRO and other organizations to ensure a thorough assessment to support the intelligence certification. As organizations formally post comments to KM/DS or JCPAT-E for the corresponding O-6/Stage I or

Flag/Stage II suspenses, intelligence reviewers will simultaneously provide intelligence related comments directly to J2P-1/IRCO for subsequent collaborative discussion throughout the community. To ensure the full range of potential intelligence supportability issues is addressed, communication and collaboration among intelligence reviewers throughout the review process is critical.

d. Criteria. Intelligence reviewers will assess both requirements *for* intelligence (such as requirements for intelligence information or services) as well as compliance with standards required *by* intelligence (such as interoperability and security) in accordance with Enclosures D, E and G. Enclosure D provides the criteria to be used as a “checklist” guide for reviewers. Enclosure E provides descriptions of the generalized intelligence support requirements identified in Enclosure D, to include general qualitative and quantitative attributes expected. Enclosure G provides reviewers with additional guidance for ICDs, CDDs, CPDs, ORD Updates/Annexes and ISPs to ensure completeness and standardization. Reviewers will forward comments directly to J2P-1/IRCO in the format prescribed by the KM/DS staffing tool, as described in detail in references b and h. Intelligence-related comments should be as specific and constructive as possible.

e. Resolving Intelligence-related Issues

(1) Time permitting, as issues are raised during the review process, J2P-1/IRCO will coordinate with the document sponsor to attempt to resolve issues at the lowest level (e.g. incomplete declaration of intelligence support requirements). Informal resolution efforts will be considered by J2P-1/IRCO but will not necessarily preclude submission of a non-concur and the need for formal comment resolution.

(2) J2P-1/IRCO will coordinate intelligence certification issues continuously with the BAWG in mutual support of the BA FCB. Intelligence support issues, especially those related to potential shortcomings in intelligence support, provide a critical input into the development of joint intelligence architecture planning and policy and support the BA FCB’s responsibility to identify, analyze, prioritize and validate capability needs in the area of intelligence. To facilitate this support, J2P-1/IRCO will provide the BAWG and the BA FCB with an Intelligence Certification Summary (see Enclosure F) summarizing the DOD-wide intelligence issues tied to a specific certification and will brief the BA FCB as required. For programs to which other FCBs have been assigned lead, J2P-1/IRCO will coordinate with other affected FCBs to ensure they are made aware of potential intelligence related issues that must be addressed and resolved.

(3) As required, J2P-1/IRCO will convene an ICWG to address and resolve outstanding intelligence support issues. The ICWG will include subject matter experts as appropriate from the combatant commands, Services, Joint Staff (J-2/J-3/J-6/J-8), defense and national intelligence agencies, ASD(NII) and USD(I) to address the issues.

(4) Intelligence certification activities seek to resolve intelligence supportability issues at the lowest level appropriate to those issues. If the intelligence certification issue cannot be resolved by the ICWG, the issue will be documented in the Intelligence Certification Summary (Enclosure F) and brought to the attention of the appropriate FCB(s). Certification failure is further addressed in paragraph 5 below.

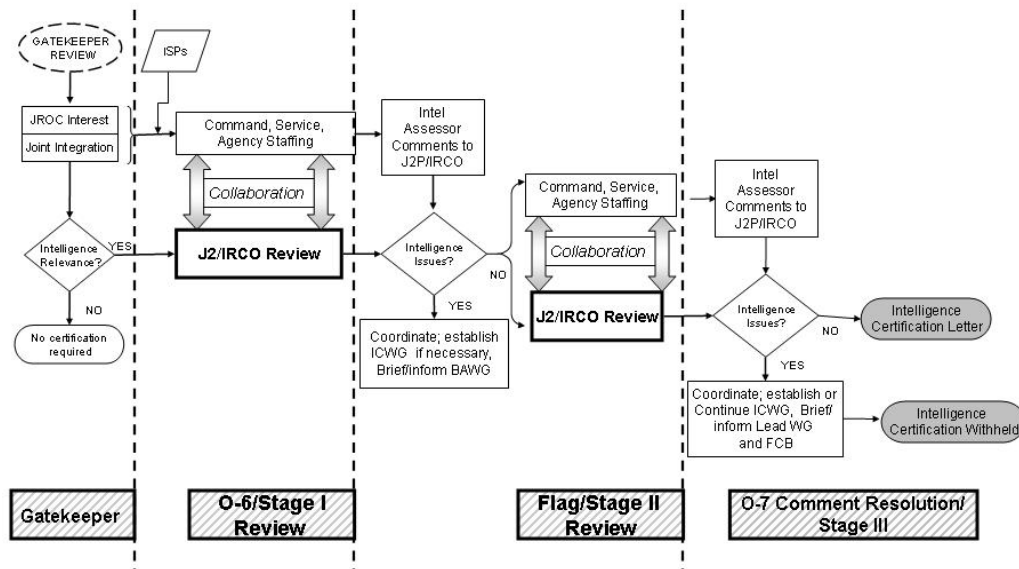


Figure B-2. Final Intelligence Certification Process

#### 4. Intelligence Certification

a. If no intelligence-related issues are identified during the course of both document reviews, or once issues are resolved through appropriate organizational bodies identified above, intelligence certification will be granted (for the specific document and associated acquisition stage). J2P-1/IRCO will post the intelligence certification letter (as illustrated in Enclosure F) to the appropriate staffing tool (KM/DS or JCPAT-E).

b. The intelligence certification affirms that:

(1) Requirements for intelligence support (using Enclosures D, E and G as guides) have been completely declared, adequately identified, and thoroughly assessed by a robust community of intelligence reviewers for projected supportability.

(2) The critical intelligence supportability or threat-related issues identified during coordination of program documents have been satisfactorily resolved through sponsor coordination or by the appropriate ICWG, FCB WG, FCB (or other appropriate body).

(3) New or revised guidance regarding the system or program's intelligence information, infrastructure or resource requirements has been incorporated into the document.

(4) Any projected shortcomings in joint intelligence support will be included in annual BAWG analysis to identify and prioritize capability gaps within the Battlespace Awareness functional area in accordance with references a, b and t.

c. Certification Interpretation. The level of intelligence support required and its associated importance can vary greatly from program to program; thus the risk associated with potential inadequate, insufficient or nonexistent intelligence support also varies. The analysis associated with the intelligence certification provides a necessary context for decision makers to assess those risks associated with the potential lack of intelligence support. In other words, it is not enough to know only that a program document failed intelligence certification; the program manager, sponsor and oversight bodies need to understand why a program failed. This context is also required to help frame shortfall mitigation strategies.

(1) Risk Assessment Variables. Unlike technical interoperability testing associated with the J-6 Interoperability Certification, the variables in the intelligence certification are often less discrete. There are two key variables associated with intelligence supportability related risk.

(a) Intelligence Dependency Level. Programs have varying degrees of reliance on intelligence support. For example, a system that requires unique, complex, dynamic intelligence-derived products in order to operate effectively has a higher intelligence dependency level than a system requiring static "one-time" intelligence support during its design phase.

(b) Intelligence Supportability Expectation. Supportability is not inherently quantifiable because it usually involves unknown or

indeterminate variables. For example, supportability of an individual intelligence information need may be tied to the best (but not definitively) known projection of future technological collection capabilities, or to an *estimated* production capacity based upon maximum potential demand level. Likewise, the complexity of associated mitigation strategies for a support shortfall will also affect the expectation of intelligence supportability. For instance, if a simple process change can remedy a particular intelligence information demand shortfall, the supportability expectation is higher. In contrast, if a mitigation strategy will require a materiel change to develop a new and technically complex capability, the supportability expectation is likely to be lower. Naturally, as the dependency and complexity levels for intelligence support increase and supportability expectations decrease, the associated level of risk also increases. Figure B-3 illustrates this concept:

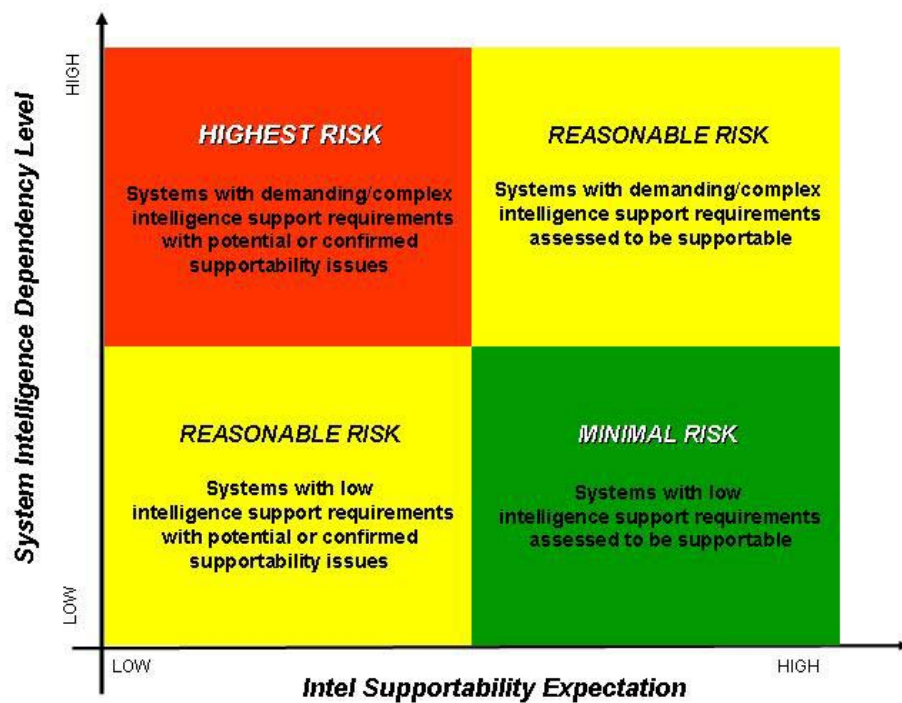


Figure B-3. Intelligence Supportability Risk Scale

The risk assessment should take into account the reasons a program's expected supportability was assessed as low (as summarized in the Intelligence Certification Summary described in Enclosure F), as well as any associated intelligence shortfall mitigation strategies in progress. It is critical that the outputs from this process directly contribute to the planners involved with intelligence architecture development, to ensure it will continue to meet the needs of the joint warfighter.

5. Certification Failure. Outstanding critical comments directly relating to the criteria contained in this instruction from reviewing organizations identified in Enclosure A will result in intelligence certification failure. For programs to which the BA FCB is assigned Lead, should J2P/IRCO receive contradicting critical comments from two or more participating organizations, the issue will automatically be deferred to the BA FCB. As discussed in paragraph 3e, comment resolution should be handled progressively, beginning with direct sponsor/commenter discussion, followed by creation of an ICWG, and then referred to the appropriate FCB if needed. Should issues remain unresolved by the FCB, the program will proceed through the JCIDS process IAW reference t.

ENCLOSURE C

INTELLIGENCE CERTIFICATION COLLABORATION MATRIX

The table below illustrates general areas of interest and expertise with respect to organizations that contribute to the intelligence certification process. It is not a tasking or responsibility matrix.

Program Characteristic	DIA/ DI	DIA/ DH	DIA/ DS	DIA/ DT	J2/ IRCO	J2/ CI	J2/ J2M	J2/ J2P 3	J2/ J2T	Services & Commands	NGA	NSA/ CSS	NRO	
Program Type														
Weapon System	A L L		AR	AR	A L L				AR	AS REQUIRED BASED ON SERVICE & COMMAND RELEVANCE	AR	AR	AR	
Combat Support			AR	AR					AR		AR	AR	AR	
Logistics			AR								AR	AR		
Weather			AR								AR	AR	AR	
Intelligence Collection		AR	AR	X		AR	AR	AR	AR		AR	AR	AR	
Automated Information System			X	AR					AR		AR	AR	AR	AR
Requires specialized Intelligence Support (Corresponding with Enclosure D and Enclosure E)														
Intelligence Manpower (1a & b)	A L L				A L L	AR				AS REQUIRED BASED ON SERVICE & COMMAND RELEVANCE	AR	AR	AR	
Intelligence Resources (2a & b)						AR					AR	AR	AR	
Collection Management (3a & b)		AR	AR	X			AR	AR			AR	AR	AR	
Signature Support/ Denial and Deception (4a & b)		X		X		AR			AR		X	X	AR	
Geospatial Intelligence (2a & b, 5a & b, 7a & b)				AR					AR		X		AR	
Targeting/BDA/MEA (2a & b, 5a & b, 6a & b)				AR				AR	X		X	AR	AR	
Combat Search and Rescue or Personnel Recovery (7a & b)												AR	X	X
Intelligence Preparation of the Battlespace (2a & b, 8a & b)				AR				AR	AR		AR	AR	AR	AR
Combating Terrorism				AR			JITF-CT				AR	AR	X	AR
Counterdrug				AR								AR	X	AR
Counterproliferation				X								AR	AR	AR
Indications and Warning (9a & b)				X				X				AR	AR	X
Space Intelligence Support (10a & b)												AR	AR	X
Counterintelligence (11a & b)		AR					X						AR	
Intelligence Training (12a & b)				AR							AR	AR	AR	AR
Dissemination Support (13a & b)			X	X				AR	AR			AR	AR	AR
IMINT				X					AR			X		X
SIGINT				AR					AR				X	X
MASINT				X					AR			X		X
Defense HUMINT		X		AR					AR					AR
TECHINT		X		X								AR	AR	AR

**Legend:** AR = As Required See Glossary for other acronyms.

(INTENTIONALLY BLANK)



ENCLOSURE D

INTELLIGENCE CERTIFICATION CRITERIA

The table on the following pages details criteria used to review, assess and certify all JCIDS documents and ISPs as detailed in Enclosure B. Should legacy C4ISPs be submitted for review, the criteria listed as applicable to ISPs in this table should be considered applicable for the legacy C4ISP document as well. For detailed descriptions of each intelligence support requirement category (e.g., Intelligence Manning, Collection Management Support), refer to Enclosure E.

	Certification Criteria	Source	R'qmt Type			Certification Criteria Category			Document Applicability						Acquisition Cycle Applicability						Primary Office of Expertise
										I C D	C D D	C P D	I S P	O R D	C R D						
REQUIREMENTS FOR INTELLIGENCE																					
THREAT VALIDATION	Has the operational environment in which the capability must be employed been addressed in general terms?	CJCSM 3170 Series	X			X			X						X						DIA/DI
	Have the organizational resources that provided threat support to JCIDS analysis and capability development been cited?	CJCSM 3170.01			X	X			X	X	X			X	X	X	X				DIA/DI
	Have current and projected threat capabilities (lethal and non-lethal) to be countered throughout the capability's lifecycle been addressed?	CJCS 3170 Series, DoDD 5000.1, DoDD 5105.21	X			X			X	X	X		X	X	X	X	X	X	X	X	DIA/DI
	For ACAT ID programs, were the the most current versions of DIA-validated threat documents used to support JCIDS analysis and documentation? For all other programs, have the most current DIA- or Service-validated threat documents been used and cited?	CJCSM 3170 Series, DoDD 5000.1, DoDD 5105.21	X			X			X	X	X		X	X	X	X	X	X			DIA/DI
	Has the threat environment, to include specific threat capabilities, the nature of the threat, and threat tactics been summarized?	CJCSM 3170 Series, CJCSI 3170.01B (for ORDs)	X			X				X	X		X	X	X	X	X	X	X	X	DIA/DI
	Are judgments or extrapolations regarding adversarial capabilities appropriate, logical, and consistent with existing, DIA-validated assessments?	DIAR 55-3	X			X			X	X	X		X	X	X	X	X	X	X	X	DIA/DI

Table D-1. Threat Validation

Certification Criteria		Source	R'qmt Type			Certification Criteria Category			Document Applicability						Acquisition Cycle Applicability					Primary Office of Expertise	
			Information Based	Resource Based	Infrastructure Based	Completeness	Supportability	Impact	I C D	C D D	C P D	C 4 I S P	O R D	C R D	Concept Refinement	Technology Development	System Development & Demonstration	Production and Deployment	Operations and Support		
REQUIREMENTS FOR INTELLIGENCE																					
INTELLIGENCE SUPPORT THROUGHOUT SYSTEM LIFESPAN	1a. Have demands on intel manpower throughout the system's lifecycle been addressed?	CJCS 3170 Series				X		X												Services, CoComs & Agencies	
	1b. Is intelligence manpower throughout the system's lifecycle (based upon projected demands) expected to be available, suitable, and sufficient throughout the program's expected lifecycle?			X			X			X	X	X	X		X	X	X	X	X		
	2a. Has resource allocation, with regard to projected intelligence support requirements, been considered (e.g., does the system have planned dependencies on currently unfunded intelligence systems or capabilities)?	CJCSI 3312.01				X		X												J2P, Services, Agencies & CoComs	
	2b. Are projected resource levels required for intel support expected to be available, suitable, and sufficient throughout the program's expected lifecycle?					X			X	X	X	X		X	X	X	X	X			
	3a. Have requirements for support from the intelligence collection management infrastructure been addressed?	CJCS 3170 Series				X															Agencies
	3b. Is the current and projected collection management infrastructure (with regard to projected demands for intelligence information) expected to be available, suitable, and sufficient throughout the program's lifecycle?			X	X		X			X	X	X	X							X	

Table D-2. Intelligence Support Criteria

	Certification Criteria	Source	R'QMT Type			Certification Criteria Category			Document Applicability						Acquisition Cycle Applicability					Primary Office of Expertise
									I C D	C D D	C P D	I S P	O R D	C R D						
INTELLIGENCE SUPPORT THROUGHOUT SYSTEM LIFESPAN, CONTINUED	4a. If appropriate, have requirements for threat or target signature support or denial and deception analysis been addressed (to include qualitative and quantitative attributes such as coverage, timeliness, content, fidelity, security, scalability and accuracy)?	CJCSM 3170 Series	X			X				X	X	X	X			X	X	X	X	DIADT, DIA/DH, J2CI, Services, Agencies, and CoComs
	4b. If so, are existing or projected intelligence products of that nature (and supporting infrastructure) expected to be available, suitable, and sufficient throughout the program's lifecycle?		X	X	X		X	X												
	5a. If appropriate, have requirements for geospatial intelligence been addressed (to include qualitative and quantitative attributes such as coverage, timeliness, security, scalability and accuracy)?	CJCSI 3901.01A, CJCSM 3170 Series	X			X				X	X	X	X			X	X	X	X	DIADT, NSA, CoComs
	5b. If so, are existing or projected geospatial intelligence (and supporting infrastructure) expected to be available, suitable and sufficient throughout the program's lifecycle?		X	X	X		X	X												
	6a. If appropriate, have requirements for targeting support (e.g., target development, mission planning support, precise positioning support, battle damage assessment support, munitions effects assessment support, weaponeering support) been addressed (to include qualitative and quantitative attributes)?	CJCSM 3170 Series	X			X				X	X	X	X			X	X	X	X	J2T, DIADT, Services, CoComs, Agencies
	6b. If so, are existing or projected targeting products or services (and supporting infrastructure) expected to be available, suitable and sufficient throughout the program's lifecycle?		X	X	X		X	X												

	Certification Criteria	Source	R'QMT Type			Certification Criteria Category			Document Applicability						Acquisition Cycle Applicability						Primary Office of Expertise		
										I C D	C D D	C P D	I S P	O R D	C R D								
INTELLIGENCE SUPPORT THROUGHOUT SYSTEM LIFESPAN, CONTINUED	7a. If appropriate, have requirements for Combat Search and Rescue/Personnel Recovery (CSAR/PR) intelligence support been addressed (to include qualitative and quantitative attributes such as coverage, timeliness, security, scalability and accuracy)?	CJCSM 3170 Series	X			X					X	X	X	X							X	Agencies, CoComs, Services	
	7b. If so, are expected CSAR or PR products and services (and supporting infrastructure) expected to be available, suitable and sufficient throughout the program's lifecycle?		X	X	X		X	X															
	8a. If appropriate, have requirements for intelligence preparation to the battlespace (IPB) been addressed (to include qualitative and quantitative attributes such as coverage, timeliness, security, scalability and accuracy)?	CJCSM 3170 Series	X			X					X	X	X	X		X	X	X	X		X	DIADI, Services, CoComs, Agencies	
	8b. If so, are expected IPB products (and supporting infrastructure) expected to be available, suitable and sufficient throughout the program's lifecycle?		X	X	X		X	X															
	9a. If appropriate, have requirements for Indications and Warning (I&W) support been addressed (to include qualitative and quantitative attributes such as coverage, timeliness, security, scalability, and accuracy)?	CJCSM 3170 Series	X			X						X	X	X	X		X	X	X			X	DIADI, J2M, NSA/CSS, CoComs
	9b. If so, are I&W products and information (and supporting infrastructure) expected to be available, suitable, and sufficient throughout the program's lifecycle?		X	X	X		X	X															

	Certification Criteria	Source	R'QMT Type			Certification Criteria Category			Document Applicability						Acquisition Cycle Applicability						Primary Office of Expertise
									I C D	C D D	C P D	I S P	O R D	C R D							
INTELLIGENCE SUPPORT THROUGHOUT SYSTEM LIFESPAN, CONTINUED	10a. If appropriate, have requirements for space intelligence support been addressed (to include qualitative and quantitative attributes)?	CJCSM 3170 Series	X			X															DIA/DI, DIA/DT, CoComs, NSA, NRO
	10b. If so, are intelligence-based Space Support products and information expected to be available, suitable and sufficient throughout the program's lifecycle?		X	X	X		X			X	X	X	X		X	X	X	X	X		
	11a. If applicable, have requirements for counterintelligence support to Research and Information Protection efforts been addressed?	CJCSM 3170 Series, DoDD 5200.39	X			X															J2/CI
	11b. If so, are counterintelligence products and information (and supporting infrastructure) expected to be available, suitable and sufficient throughout the program's lifecycle?		X	X	X		X	X		X	X	X	X			X	X	X	X		
	12a. Has projected support for intelligence training requirements (manpower, materials, facilities, equipment) for both initial system standup and sustainment of intelligence skills for the life of the system been addressed?	CJCSM 3170 Series			X	X				X	X	X	X				X	X			Services, Agencies, CoComs, J-2
	12b. Is intelligence training support (and supporting infrastructure) expected to be available, suitable and sufficient throughout the program's lifecycle?		X	X			X	X													
	13a. Have dissemination support requirements (as described in Enclosure E) been addressed?	CJCSM 3170 Series			X	X															DIA/DS, DIA/DT, J2P-3, CoComs, Agencies
	13b. Is intelligence dissemination infrastructure (based upon projected joint/IC demands) expected to be available, suitable and sufficient throughout the program's expected lifecycle?				X		X	X		X	X	X	X		X	X			X		

	Certification Criteria	Source	RQMT Type			Certification Criteria Category			Document Applicability						Acquisition Cycle Applicability						Primary Office of Expertise
			1	2	3	1	2	3	1	2	3	4	5	6	1	2	3	4	5	6	
REQUIREMENTS BY INTELLIGENCE																					
INTEROPERABILITY	Is the system expected to use TS/SCI traffic systems, and if so, will the end-to-end capability be compliant with DCI security directives and will the communication interface be technically compatible and compliant with DoD Intelligence Information System (DODIIS) standards?	DCID 6/3, DCID 6/9	X		X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	DIA/DS
	Is the system expected to interface with foreign or coalition Information Systems, and if so, has management & control of information been addressed?	DOD 14630.8, DoDD 8500.1	X		X	X		X		X	X	X	X				X	X	X		DIA/DS, CoComs, Services
	Have intelligence handling requirements, intel-related information system requirements, standards, or architectures been considered?	DODD 8500.1, DCID 6/9, CJCSI 6212 Series			X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	DIA/DS, NSACSS, Services
	Are there any outstanding interoperability issues related to the Joint Intelligence Interoperability Board's (JIIB) Joint System Baseline Assessment (JSBA) that could affect overall supportability of the system in question?	JIIB Business Plan		X	X		X	X		X	X	X	X			X	X	X	X		DIA/J2P-3
	If the capability involves development of an intelligence information system or exchanges data within Intelligence Community shared spaces, does it mandate the use of Extensible Markup Language (XML) for metadata tagging and markup?	IC Policy for Metadata & Metadata Markup		X	X		X	X		X	X	X	X			X	X	X	X		DIA/J2P-3, J2P-1/IRCO
	If the capability has or will introduce new metadata standards, have or will they be registered with the Intelligence Community Metadata Repository (ICMR)?	IC Policy for Metadata & Metadata Markup		X	X		X	X		X	X	X	X			X	X	X	X		DIA/J2P-3, J2P-1/IRCO

Table D-3. Interoperability Criteria

	Certification Criteria	Source	R'QMT Type			Certification Criteria Category			Document Applicability						Acquisition Cycle Applicability						Primary Office of Expertise
										I C D	C D D	C P D	I S P	O R D	C R D						
REQUIREMENTS <i>BY</i> INTELLIGENCE																					
SECURITY	If the system is expected to use TS/SCI information, have physical security needs been addressed (e.g. use of a Special Compartmented Information Facility)?	DCID 6/3, DCID 6/9		X	X	X					X	X	X	X						X	DI/ADS
	Is the system expected to use TS/SCI traffic systems, and if so, will the end-to-end capability be compliant with DCI security directives and will the communication interface be technically compatible and compliant with DoD Intelligence Information System (DODIIS) standards?	DCID 6/3, DCID 6/9	X		X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	DI/ADS
	Is the system expected to interface with foreign or coalition Information Systems, and if so, has management & control of information been addressed?	DOD 14630.8, DoDD 8500.1	X		X	X		X		X	X	X	X				X	X	X		DI/ADS, CoComs, Services
	For systems for which intelligence authorities are the designated accrediting authorities, have security testing considerations been addressed in interoperability testing plans?	CJCSI 6212.01C		X	X	X					X	X	X	X					X	X	DI/ADS, Agencies

Table D-4. Security Criteria



	Certification Criteria	Source	RQMT Type			Certification Criteria Category			Document Applicability						Acquisition Cycle Applicability						Primary Office of Expertise	
										I C D	C D D	C P D	I S P	O R D	C R D							
REQUIREMENTS BY INTELLIGENCE																						
CONSISTENCY WITH JOINT INTELLIGENCE POLICY, STRATEGY, DOCTRINE, GUIDANCE, AND ARCHITECTURE PLANNING	If the capability in development will provide or enable intelligence collection, tasking, processing, exploitation, dissemination or production, do required attributes for capability definitions contain appropriate measures of effectiveness (e.g. time, distance, effect [including scale]) and obstacles to overcome?	CJCSM 3170 Series	X	X	X			X	X							X	X	X	X	X	J2P/IRCO, BAWG	
	Is the capability expected to contribute anything new to the existing or currently planned Battlespace Awareness Joint Functional Concept (JFC) and integrated architecture? If so, is the addition assessed to be easily absorbed and integrated, or will the additional input likely require significant materiel and/or DOTMLPF changes? Will timing of expected changes support the capability's projected IOC? If not, has a mitigation plan been addressed?	CJCSI 3312.01, BA JFC	X	X	X			X	X	X	X	X	X	X	X	X	X	X		X	J2P/IRCO, BAWG	
	Is the capability expected to require new , unique and unplanned support or additional, existing support (as projected by the intelligence architecture)? If so, is the additional support assessed to be easily provided, or will the additional support likely require DOTMLPF changes?	CJCSI 3312.01, BA JFC	X	X	X			X	X	X	X	X	X	X	X	X	X	X		X	ALL	

Table D-5. Consistency with Joint Intelligence Policy, Strategy, Doctrine, Guidance and Architecture and Planning

(INTENTIONALLY BLANK)

ENCLOSURE E

INTELLIGENCE SUPPORT REQUIREMENT CATEGORY  
DESCRIPTIONS

This enclosure provides document drafters descriptions of generalized intelligence support requirement categories (that numerically correspond with criteria listed under the “Intelligence Support Throughout System Lifespan” section in Enclosure D) to help identify intelligence support needs. These descriptions are not all-inclusive and should be tailored to each individual program. In addition, generic operational capabilities with which the support requirements are usually associated, as well as generalized quantitative and qualitative attributes, are discussed. With regard to quantitative attributes, not all types of intelligence support can be discretely quantified. The purpose of requiring that quantitative levels of support be addressed is simply to provide some relative measure of effectiveness or demand level to assess supportability of those needs. If and when specific metrics can be defined for qualitative attributes, they will be included in future iterations of this instruction. If applicable, supported Universal Joint Task List tasks (reference p) are indicated in parentheses following the support requirement description.

1. Intelligence Manpower. This requirement category should be addressed if either the operational capabilities of the program or required support capabilities will require intelligence personnel for any and all phases (to include development, testing, training and operation) of the program’s life cycle. Depending on the maturity of the program, a Manpower Estimation Report (MER) may or may not have been accomplished; once accomplished, intelligence implications from that report should be included in the applicable CDD or CPD. (SN 4.1.1)

*Associated generic capabilities:* Potentially all.

*Qualitative Attributes:* Address whether existing specialties suffice, or if specific skills are required for support. Address whether specialized training of personnel will be required.

*Quantitative Attributes:* Address whether manpower requirements will be transparent (i.e., existing organizations and billets will provide support) or will require additional, dedicated intelligence personnel.

2. Intelligence Resource Support. This requirement should be addressed if either the operational capabilities of the program or required support capabilities will require or depend upon intelligence funding (such as the

General Defense Intelligence Program [GDIP], the National Foreign Intelligence Program [NFIP], Joint Military Intelligence Program [JMIP] or the Tactical Intelligence and Related Activities [TIARA] funding). In particular, if the program will depend upon intelligence capabilities or systems that are not yet programmed, these dependencies should be identified.

*Associated generic capabilities:* Potentially all.

*Qualitative Attributes:* N/A.

*Quantitative Attributes:* Address to what extent the program depends upon non-funded programs (is it dependent upon “To-be” elements?).

3. Collection Management Support. The requirement for collection management support refers to both management of collection assets as well as identification and management of intelligence information requirements. The collection management process converts intelligence information requirements into operational requirements for assets to collect information. At the strategic and operational level, collection management support refers to the personnel, expertise and systems required to ensure intelligence collection assets (e.g., national, joint, coalition, multinational) are effectively employed. At the tactical level, collection management support refers to the personnel, expertise and systems required to ensure intelligence information needs are submitted through the appropriate requirements channels. As the net-centricity of the joint force increases, this may come in the form of ensuring “subscriptions” are adequately defined to ensure receipt of needed intelligence information. (ST 2.1.2, ST 2.1.3, OP 2.1.3, OP 2.1.4)

*Associated generic capabilities:*

- Intelligence collection assets.
- Intelligence collection management assets.
- Intelligence operations, tactics, techniques and procedures (TTPs).
- Assets involving (strategic) decision-making functions.
- Programs with intelligence information needs to support their operation(s).

*Qualitative Attributes:* Level of training required for personnel, system knowledge required, level of national/coalition interoperability to enable timely intelligence collection management.

*Quantitative Attributes:* Address to what extent the program will have intelligence information needs during operation. Address whether support provided will be direct or via reach-back.

4. Signature Support/Denial and Deception Analytical Support.

Signature data consists of the sum of data measurements associated with a specific target (equipment/location/event) and may be used by intelligence analysts, automated sensors as well as system design and development engineers. For example, with respect to automated sensing, signature support is required when system sensors must match collected data against signature templates automatically, accurately and dynamically under differing atmospheric and environmental conditions (one example is assisted target identification, recognition or classification). Signature support may come in the form of the collection and measurement of physical data describing specific equipments, events and locations as well as the algorithms required to make those data useful and actionable (e.g., automatic target cueing and automatic target recognition [ATC/ATR]). (SN 1.1.6, SN 2.2.1, SN 2.2.2, SN 2.3.1, SN 2.4.1, SN 2.4.1.2, ST 2.2.1, ST 2.3.1, ST 2.3.2, ST 2.3.3, ST 2.4.1.1, ST 2.4.2.4, ST 2.4.2.5, OP 2.2.1, OP 2.2.4, OP 2.3.1.1, OP 2.4.1.1, OP 2.4.2.3, OP 3.4.1, OP 3.4.2, OP 5.1.11, OP 6.1.11, OP 6.2.11)

*Associated generic capabilities:* Assets required to detect, identify, classify or characterize objects in the battlespace.

*Qualitative Attributes:* Format, content, reliability, data fidelity, accuracy, timeliness, scalability, static versus dynamic data, spectral (frequency) range required, specific target types to be detected, identified or characterized; level of automation and data fusion required, compliance with National Signature Program (NSP) standards.

*Quantitative Attributes:* Volume of data required.

5. Geospatial Intelligence and Services Support. “Geospatial intelligence” means the exploitation and analysis of imagery and geospatial information to describe, assess and visually depict physical features and geographically referenced activities on the earth. Geospatial intelligence consists of imagery, imagery intelligence and geospatial information. This intelligence support category, “Geospatial Intelligence and Services Support” refers to a program’s need for a geospatial intelligence product, piece of geospatial intelligence information or associated geospatial intelligence service that is needed to support the accomplishment of a specific mission. The supported mission can include deliberate and crisis planning, force or system development,

training or routine operations. Geospatial intelligence support during development of a system may include prototyping of products and services unique to the system, which can directly affect NGA capabilities. Essential geospatial intelligence support during operations and sustainment, on the other hand, is based on deployment footprints and primarily affects capacity of NGA and its mission partners. Both qualitative and quantitative requirements must be estimated in advance to ensure effective geospatial intelligence support across the system lifecycle. Specific products may include aeronautical products, imagery products, point positioning support (may come from various sources), and digital features or terrain elevation data produced by the NGA. (ST 2.2.3, ST 2.4, OP 2.4)

*Associated generic capabilities:* Potentially all.

*Qualitative Attributes:* Required datums, coverage, scalability, timeliness, formats, accuracy, resolution level (e.g., imagery and/or Digital Terrain Elevation Data [DTED] levels). Compliance with NGA standards is a mandatory requirement. Note: For coordinate accuracy, see the targeting description below.

*Quantitative Attributes:* Addresses the numeric quantity of products, demand levels for services.

6. Targeting Support. Targeting (in general) refers to “the process of selecting and prioritizing targets and matching the appropriate response to them, taking account of operational requirements and capabilities” (Joint Publication 2-01.1, “Joint Doctrine for Intelligence Support to Targeting”). Within the context of this instruction, the requirement for targeting support refers to a wide array of intelligence information, products or services throughout all levels of warfare--and, for the purposes of the intelligence certification--throughout all phases of the acquisition cycle.

a. Target intelligence support may be required during munition design, development and testing to help ensure expected munition lethality. Munitions Effects Assessment (MEA) and Battle Damage Assessment (BDA) studies may help identify initial gaps in force application capabilities.

b. During the operational and sustainment phases of acquisition, targeting support refers to the intelligence information, infrastructure or resources required:

- To support commanders' development of objectives, guidance and intent;
- For target development (to include derivation of coordinates), validation, nomination and prioritization;
- To support planners at national, strategic and tactical/operational levels;
- To support capabilities analysis and force assignment;
- To support mission planning and execution (e.g., mission planning support such as weaponeering, target imagery notation, and coordinate verification at the unit levels);
- To support operational execution (e.g., time-sensitive targeting support such as target identification, coordinate derivation and weaponeering)
- And to support the combat assessment process (to include BDA, MEA and supporting re-attack recommendations).

c. Examples of targeting products include target lists, target folders, target materials, modeling and simulation products, collection and exploitation requirements to support targeting and target briefs. Examples of targeting services include weaponeering, casualty and collateral damage estimation, point positioning/coordinate mensuration and verification and tactical mission planning support. (SN 2.4.1.3, SN 2.4.2.4, SN 3.2.1, SN 3.2.5, SN 3.3.5, ST 2.2.1, ST 2.4.2.4, OP 2.2.5, OP 2.4.2.4, OP 3.1.3, OP 3.1.4, OP 3.1.6.1, OP 3.1.6.2, OP 3.1.6.3)

Note: Targeting support may overlap with the Geospatial Intelligence and Services Support Requirement; many targeting services rely upon and/or incorporate geospatial products or information.

*Associated generic capabilities:* Systems that will perform or manage the application of force or the conduct of information operations.

*Qualitative Attributes:* Qualitative attributes will vary greatly by specific products required, but examples could include format specifications, accuracy requirements and timing requirements. Coordinate seeking weapons or weapons that can or will be able to operate in a coordinate seeking mode must declare required Target Location Error (TLE) expressed as circular and linear error) in meters or feet) with associated confidence level.

*Quantitative Attributes:* Quantitative attributes will also vary greatly by specific product or service required but could refer to volume of targets managed and numbers of target folders produced, numbers of missions and associated targets or aimpoints to plan for during mission planning.

7. Combat Search and Rescue Intelligence Support. Combat search and rescue (CSAR) (in general) refers to a specific task performed by rescue forces to affect the recovery of distressed personnel during war or military operations other than war (JP 3-50.2, "Doctrine for Joint Combat Search and Rescue"). Intelligence plays a vital role in the planning and conduct of CSAR operations; in fact "the enemy threat will have the greatest impact on search criteria and the method of recovery to be used." (JP 3-50.2)

Due to the sensitivity, inherent jointness and time-sensitive nature of most CSAR operations, there are usually unique intelligence support requirements such as:

- Understanding Joint CSAR TTPs.
- Familiarity with selected areas for evasion, contact points and helicopter landing zones.
- Familiarity with procedures for facilitating national intelligence support to CSAR operations.
- Understanding extensive communication methods, means and procedures throughout the tactical, operational and strategic levels.
- Understanding and documenting the particular and discrete signature data associated with specific CSAR events.

(SN 2.2.1, SN 2.3.1, SN 2.4.1, ST 2.1.3, 2.2.1, ST 2.3, ST 2.4.1.1, ST 2.5, OP 2.1.3, OP 2.2.1, OP 2.3, OP 2.4.1.1, OP 2.5.3, OP 6.2.9)

*Associated generic capabilities:* Platforms/capabilities with a CSAR mission.

*Qualitative Attributes:* Accuracy, timeliness, training levels, timely reachback and integration with national and/or joint intelligence assets and capabilities.

*Quantitative Attributes:* Will most likely be tied to intelligence manpower requirements and degree to which CSAR is the platform's primary mission.

8. Joint Intelligence Preparation of the Battlespace/Intelligence Preparation of the Battlespace (JIPB/IPB) Support. In the most basic and general sense, IPB refers to intelligence analysis that depicts the battlespace and subsequently projects possible enemy courses of action. Naturally, the complexity associated with this type of support varies substantially based upon the scope of the battlespace involved. Joint Publication 2-01.3, 24 May 2004, "Joint Tactics, Techniques, and



Procedures for Joint Intelligence Preparation of the Battlespace,” defines JIPB as “what allows Joint Force Commanders and their staffs to visualize the full spectrum of adversary capabilities.” IPB has narrower scope and is focused on individual air, ground, maritime or space operations. Likewise, JIPB and IPB performed in support of transnational operations (such as counterdrug operations) may significantly differ in relative purpose and focus. This definition could therefore encompass a wide variety of specific intelligence information or products. The three transnational IPB Support subcategories are listed below:

- Combating Terrorism Analysis Support
- Counterdrug Analysis Support, and
- Counterproliferation/Chemical, Biological, Radiological, Nuclear and High Explosive (CBRNE) Analysis Support

As with all intelligence support categories, IPB support can apply throughout all phases of the acquisition cycle. An example is ensuring that acquisition programs are conceived, developed and designed with the most current and validated information on adversarial capabilities falls under this umbrella. (Note: This is also required for the formal threat validation granted by DIA). Likewise, ensuring platforms operating within the battlespace are provided with accurate and timely order of battle data and assessments of adversarial intentions, tactics and capabilities before and during operational missions falls under this umbrella. (SN 2.2.1, SN 2.2.2, SN 2.3.1, SN 2.4.1, SN 2.4.1.1, SN 2.4.1.2, ST 2.1.3, ST 2.2.1, ST 2.3.1, ST 2.3.2, ST 2.3.3, ST 2.4.1.1, ST 2.4.1.2, ST 2.4.2.1, ST 2.4.2.2, ST 2.4.2.3, ST 2.4.2.5, ST 2.5, OP 2.1.3, OP 2.2.1, OP 2.3, OP 2.4.1.1, OP 2.4.1.2, OP 2.4.2.1, OP 2.4.2.4, OP 2.5, OP 6.1.6, OP 7.2, OP 7.3)

*Associated generic capabilities:* With regard to threat support to pre-operational phases of acquisition, this requirement will apply to almost any proposed system (to include open-architecture information technology systems). With regard to IPB Support needs during operation, the requirement will apply to any platform physically operating in the battlespace. With regard to the IPB Support Subcategories, these would apply to specialized platforms or sensors tailored for such missions.

*Qualitative Attributes:* Accuracy, timeliness, frequency, format, latency, types of threat information required.

*Quantitative Attributes:* Addresses the numeric quantity of products, demand levels for services.

9. Warning Support. In a defense-related context, warning is the responsibility military intelligence has to communicate information about a developing threat to a decision maker in order to avoid surprise. Avoiding surprise requires the information be conveyed in sufficient time to allow action or reaction required to preclude, dissuade, deter or defeat emerging (future) threats.

a. Warning support--namely "Indications and Warning"--usually conveys strategic intelligence analysis supporting high-level decision makers in an operational (vice pre-operational acquisition phase) context. For the purposes of this instruction, warning support must be thought of as a type of support that occurs throughout all phases of acquisition and employment.

b. Warning support provided prior to the operational phase of acquisition may be thought of as information required by an acquisition program in order for that program to remain scientifically and technologically superior relative to the developing or projected capabilities of foreign adversaries. For example, DIA's Defense Warning Office and the Service Intelligence Centers (i.e., National Air and Space Intelligence Center, National Ground Intelligence Center, Office of Naval Intelligence, Marine Corps Intelligence Activity) provide this type of support. The ability to *provide* this support, however, depends upon direct involvement of the program manager in terms of identifying Critical Intelligence Categories (CICs). CICs refer to general or specific adversarial capabilities that, if developed, procured or implemented could significantly influence the effective operation of the developed/developing US capability. CICs then support the development of intelligence production requirements (and subsequently intelligence collection requirements) in support of that acquisition program.

c. Warning support provided once a program enters initial operating capability, *additionally\** refers to programs that require specific intelligence-derived products that provide forewarning of specific, imminent, hostile events. For additional detail regarding this type of support, refer to the DOD Indications and Warning System Operations Manual (U), J2M-0177-01-96, SECRET//US ONLY, January 1997 which may be found on Intelink through the Joint Worldwide Intelligence Communications System (JWICS) at [http://delphi.dia.ic.gov/intel/j2/j2m/pubs/J2M-0177-01-96/J2M-0177-01\\_cov.html](http://delphi.dia.ic.gov/intel/j2/j2m/pubs/J2M-0177-01-96/J2M-0177-01_cov.html).

(SN 2.2.1, SN 2.3.1, SN 2.4.1.1, SN 2.4.1.2, SN 2.4.2.1, SN 2.4.2.5, SN 3.4.2, ST 2.2.1, ST 2.3.1, ST 2.4.1.1, ST 2.4.1.2, ST 2.4.2.1, ST 2.4.2.2,

ST 2.4.2.5, OP 2.1.3, OP 2.2.1, OP 2.3.1, OP 2.4.1.1, OP 2.4.1.2, OP 2.4.2.1, OP 2.5.3, OP 6.1.6, TA 2.4)

\* Warning support with regard to CICs is continued throughout a program's life cycle.

*Associated generic capabilities:* Potentially all.

*Qualitative Attributes:* Accuracy, timeliness, format, frequency, communication means.

*Quantitative Attributes:* This type of support is impossible to accurately quantify but may at least be generally addressed in terms of high, medium or low demand levels. Depending on the technological complexity of the program, the level of warning support required may vary. The numbers of CICs developed may be a good indicator of the quantitative levels of support required. For operational warning support, warning support demand levels will vary by the primary mission of the program. For example, command and control programs will tend to require more operational warning support than an autonomous munition.

10. Space Intelligence Support. Space intelligence support refers to intelligence information, infrastructure or resources that provide space-specific intelligence analysis on foreign space capabilities. (Joint Publication 3-14, *Joint Doctrine for Space Operations*) (SN 3.5.1, SN 3.5.2.1)

*Associated generic capabilities:* Space-based programs; platforms that require visibility into the foreign space picture; platforms that perform space control or space support.

*Qualitative Attributes:* Accuracy, timeliness, frequency, format, latency, types of threat information required.

*Quantitative Attributes:* Addresses the numeric quantity of products, demand levels for services.

11. Counterintelligence Support. Counterintelligence refers to information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or terrorism conducted by or on behalf of foreign governments, or elements thereof, foreign organizations, foreign persons or international terrorist activities (derived from Joint Publication 2-01, 20 November 1996, "Joint Intelligence Support to Military Operations"). In the context of this

instruction, counterintelligence support (CI support) refers to the intelligence information, infrastructure or resources used to educate acquisition communities on those threats. CI support also helps those communities establish plans, tools or techniques for protecting designated science and technology information and critical program information (CPI) from such threats in accordance with reference v.

As with other requirements, counterintelligence support can and should apply throughout a program's entire life cycle. CI support may refer to providing threat awareness education to scientists and engineers performing fundamental research, to the implementation of a program protection plan. (SN 2.2.1, SN 2.3.1, SN 2.4.1.2, SN 2.4.2.5, SN 3.4.6, ST 2.2.1, ST 2.3, ST 2.4.1.1, ST 2.4.1.2, ST 2.4.2.5, ST 2.5, OP 2.2.1, OP 2.3, OP 2.4.1.1, OP 2.4.1.2, OP 2.5, OP 6.2.11, OP 6.2.12, OP 6.3.14, OP 6.3.2, OP 6.6)

*Associated generic capabilities:* Potentially all.

*Qualitative Attributes:* Format, training level of CI personnel involved, timeliness requirements, compliance with reference v.

*Quantitative Attributes:* General level of effort required (1 person? 10 people?)

12. Intelligence Training Requirements. Some programs may require specialized training of the intelligence personnel supporting a program. The requirement may be for additional personnel trained by existing training programs or for additional personnel as well as a new, unique training program that is yet to be developed. In either case, the requirement for specific training of intelligence personnel required to support any phase of a program's life cycle must be declared. (SN 4.1.2)

*Associated generic capabilities:* Potentially all.

*Qualitative Attributes:* Certifications required, skill specialties required (e.g., Air Force Specialty Code, Military Occupational Specialty), schools/courses required, language skills.

*Quantitative Attributes:* Will be tied to manpower (and subsequent training requirements) once known.

13. Dissemination Support. Although the movement toward net-centricity and "plug-and-play" networks has, to some extent, reduced the technical challenges of information dissemination, intelligence infrastructure (such as intelligence networks, systems and software) and

resources (such as funded programs or manpower) are still critical enablers of information delivery. One measure of determining dissemination support needs is to examine relevant crosswalks with key intelligence CRDs (soon to be converted to Mission Area [MA] ICDs IAW reference u) listed below (ST 2.5, OP 2.5):

- Distributed Common Ground/Surface Systems (DCGS) CRD, 6 January 2003
- Imagery and Geospatial Information (IG) CRD, 15 June 2000
- Unified Cryptologic System (UCS) Common CRD, 25 September 2001
- Signals Intelligence (SIGINT) CRD, 7 January 2003
- US MASINT System (USMS) CRD, 14 November 2002

Another measure of dissemination support is compliance with IC and DOD data and metadata standards.

*Associated generic capabilities:* Systems/capabilities that provide intelligence information.

*Qualitative Attributes:* CRD or MA ICD and IC or DOD data and metadata standards dependent.

*Quantitative Attributes:* CRD or MA ICD and IC or DOD data and metadata standards dependent.









(INTENTIONALLY BLANK)

ENCLOSURE F

INTELLIGENCE CERTIFICATION SUMMARY AND LETTER

The slide below is a notional example of information to be presented at BAWG and BA FCB meetings (and other FCBs as appropriate) to highlight intelligence related issues identified as a result of the Intelligence Certification. Red markings indicate a critical comment was made in the designated criteria category; yellow indicate substantive issues, and green indicate administrative only or no comments in a particular criteria category (as identified in Enclosures B and D).

UNCLASSIFIED

Intelligence Certification Summary			
Program: Program Name		Date: XXXXXXX	
Certification Status:	CONCUR	X CONCUR WITH COMMENT	NON-CONCUR
Certification Criteria:	Completeness	Supportability	Impact
			
Issue Summary			
Threat Validation:			
1. Threat references are not complete. (Substantive/Completeness)			
2. DIA-validated threat references were not used and this is an ACAT ID program. (Substantive/Supportability)			
Intelligence Support:			
1. No USMS CRD Crosswalk. (Substantive/Completeness)			
Interoperability:			
1. Program will generate new metadata standards that have not been registered with the IC or DoD XML registries. (Substantive/Supportability)			
Security:			
Intelligence Architecture Impact:			
1. JWICS bandwidth limitations may preclude meeting Objective performance. (Substantive/Supportability & Impact)			

UNCLASSIFIED



THE JOINT STAFF  
WASHINGTON, DC

Reply ZIP Code:  
20318-2000

U-00XX-200X/J2P  
{date will go here}

MEMORANDUM FOR VDJ8 and <<Lead FCB>>

Subject: Intelligence Certification of <<Document Name>> (KM/DS Control  
Number: XX-XXXXXX) [stage III RMDs #]

1. Intelligence certification is granted for the <<Document Name>> written in preparation for the <<Milestone>> decision as required by CJCSI 3170.01 D, *Joint Capabilities Integration and Development System* and in accordance with CJCSI 3312.01, *Joint Military Intelligence Requirements Certification*. This certification affirms that:

a. Requirements for intelligence support have been completely declared, adequately identified and thoroughly assessed for projected supportability, and that critical intelligence-related issues identified during the intelligence certification process have been satisfactorily resolved.

b. If needed, new or revised guidance regarding the program's intelligence support needs has been incorporated into the document.

c. Any projected shortcomings in joint intelligence support identified through this process will be passed to the Battlespace Awareness Functional Capability Board for incorporation into annual analysis of capabilities and capability gaps in the Battlespace Awareness functional area as required by the CJCS 3170 Series.

2. DIA threat validation (required for the intelligence certification) is also granted for the subject document. This affirms that DIA/DI validates the projected threat environment depicted in the subject document.

3. My point of contact on this issue is <<J2P/IRCO Lead, (703) 6XX-XXX, DSN 69X-XXXX>>.

ROBERT B. MURRETT  
Rear Admiral, USN  
Vice Director for Intelligence, J2

Example of Intelligence Certification Letter



## ENCLOSURE G

### PROGRAM DOCUMENT GUIDANCE

1. Purpose. This enclosure expands on explicit and implicit drafting guidance for program documents as already provided in references b (for ICDs, CDD and CPDs), h (for ISPs) and o (for ORD updates and annexes) regarding incorporation of intelligence support requirements into program documentation. This enclosure should also guide intelligence certification reviewers with a standardized paragraph by paragraph checklist to ensure the completeness of each program document with respect to intelligence concerns.
2. General. Several references (a, b, d, f, g, h) clearly address the importance of addressing a capability's expected information needs. In addition, there are several measures by which the planned *exchange* of information is carefully examined (such as development of the Net-Ready Key Performance Parameter (NR-KPP) and the IT and NSS Interoperability and Supportability Certifications). Although intelligence is a sub-category of "information" and the associated exchange of intelligence information is important, if the information cannot be initially delivered to a sending node, the exchange capability quickly becomes ineffective. The ability to initially *deliver* intelligence information to a sending node depends upon the supporting infrastructure and resource elements of the associated intelligence community. As information needs are developed throughout the JCIDS and associated ISP processes, this concept must be kept in mind.
3. Leverage the Information Support Plan Process. Although the ISP is not considered a JCIDS document (it is required by ASD(NII), not the JROC), the outputs from the Information Needs Discovery and Analysis Process detailed in reference h (Enclosure 4) can help a sponsor address requirements for intelligence support in concurrently developed CDDs and CPDs. These intelligence information needs (and associated exchange requirements) must be clearly illustrated in architecture graphics within JCIDS documents. In accordance with references b, h and this instruction, the CDD and ISP drafting processes should extensively leverage each other.
4. Joint Capabilities Integration and Development System Document Development. While the fifth paragraph of ICDs (Threat/Operational Environment) and the fourth and ninth paragraphs (Threat Summary and Intelligence Supportability, respectively) of CDDs and CPDs are the most explicit sections (in JCIDS documents) to address intelligence

support needs, there are several other paragraphs that should refer to intelligence support or integration concepts (if applicable). The tables beginning on the following page will identify specific areas, by document type and paragraph, the sponsor should consider with respect to intelligence support. Although the intelligence considerations for CDDs and CPDs are listed in the same table, expectations with regard to specificity and detail will increase substantially for CPDs. Italicized considerations in Tables G-1 and G-2 should be addressed by all programs that contribute to Battlespace Awareness; non-italicized considerations apply to all programs. Additional formatting and development guidance for the Intelligence Supportability paragraph (paragraph 9 in CDDs and CPDs) immediately follows the tables.

Para	Para Title	ICD Consideration
1	Joint Functional Area	If the capability falls within the scope of the Battlespace Awareness (BA) functional area, or will require significant support from Battlespace Awareness elements, "Battlespace Awareness" should be listed as a Joint Functional Area/Concept (JFA/JFC).
2	Required Capability	Address whether the desired capabilities described relate to any of the key intelligence CRDs/MA ICDs (Distributed Common Ground/Surface System [DCGS], Imagery and Geospatial Intelligence [IG], the United States MASINT System [USMS], Signals Intelligence (SIGINT) or the Unified Cryptologic System [UCS]). Ensure the scope of the capability reflects the adequate degree of jointness.
3	Concept of Operations	<i>Ensure operational contributions to Battlespace Awareness efforts are clearly addressed.</i> Address whether there are any key intelligence-based capabilities required to <i>enable</i> the operational capability in achieving its desired operational outcomes.
4	Capability Gap	<i>Ensure related Battlespace Awareness capability gap(s) has (have) been clearly identified. Ensure the documented FAA and FNA analysis reflects the linkage between the identified gaps and relevant JOCs, JFCs, JICs, and integrated architectures. Ensure capability definitions contain the required attributes with appropriate measures of effectiveness and "obstacles to overcome." In other words, are the needed capabilities defined enough to convey what's needed to satisfy the capability gap?</i>
5	Threat/Operational Envt	See all threat questions under "Threat validation" as they apply to the ICD IAW Enclosure D of this instruction.
6	Functional Solution Analysis	Address whether any intelligence-based DOTMLPF aspects were analyzed. <i>Ensure all materiel and non-materiel solutions considered during the FSA are adequately identified in this paragraph. Ensure the FSA efforts and documentation reflect that community expertise has been adequately leveraged. Ensure the Analysis of Materiel Approaches reflect JROC-approved key attributes and metrics (e.g. persistence, agility, precision, reach) as documented in the BA Functional Concept.</i>
7	Final Materiel Recomm.	Ensure the analysis for the best materiel approach is commensurate with standards IAW CJCSM 3170.01A. Ensure the key boundary conditions described for the performance of the AoA reflect a thorough understanding of the functional and operational areas to include applicable threat considerations or intelligence support capabilities (i.e. ISR enablers).
App A,	OV-1	Ensure high-level intelligence systems connectivity and interoperability are accurately illustrated. Ensure the OV-1 illustration is consistent with the Concept of Operations described in Paragraph 3, and that, if appropriate, the BA functional concept and future/projected integrated architectures are referenced.

Table G-1. ICD Intelligence Considerations

**Para Para Title CDD and CPD Consideration**

1	Capability Discussion	a. Address how the capability relates to the BA functional concept, to include BA in a supporting role.
		b. <i>Ensure the capability gap is adequately addressed in terms of mission area, relevant range of military operations, and timeframe under consideration. Ensure how the current increment contributes to the required BA capability in terms of the JROC-approved key BA attributes and metrics (e.g. persistence, agility, precision, reach) documented in the BA Functional Concept. Ensure the source ICD, MA ICD, related CDDs, CPDs, and/or integrating DOTMLPF changes are identified.</i>
2	Analysis Summary	<i>For BA capabilities, ensure the summary of analysis includes the alternatives considered, objectives, criteria assumptions, conclusions, and overall recommendation. Ensure the proposed approach is not duplicative with existing or other developing joint capabilities.</i>
3	Concept of Operations Summary	Address whether there are any key intelligence support capabilities required to enable the operational capability within the context of the Concept of Operations (CONOPS). Ensure the CDD/CPD addresses the employment of the proposed solution within the context of the CONOPS.
4	Threat Summary	See all threat questions under "Threat validation" as they apply to CDDs and CPDs IAW Enclosure D of this instruction.
5	Program Summary	Address whether any undeveloped (or underdeveloped) intelligence technologies or the retirement of existing intelligence programs has affected the incremental delivery plan. In other words, address the intelligence drivers to the incremental delivery plan such as technology development, other systems in the FoS or SoS, or inactivation of legacy intelligence systems.
6	System Capabilities Required	a. Identify attributes and Key Performance Parameter (KPP) that are driven by needs for intelligence support. Ensure that objective and threshold values for attributes are supported by analysis.
		b. <i>Ensure the rationale for each KPP complies with the applicable JROC-approved intelligence CRDs/MA ICDs or reflects the insights identified in the Battlespace Awareness integrated architecture (when it becomes available). Ensure the CDD/CPD accurately captures the desired capabilities in the applicable ICD or MA ICD(s).</i>
7	FoS/SoS Synch	<i>For BA capabilities that are part of a FoS/SoS, ensure this section cites related JCIDS documents and existing capabilities. Ensure dependencies between these capabilities are defined (e.g. information exchange) and are consistent with the related documents. Ensure the CDD/CPD accurately captures the desired capabilities described in applicable CRDs or MA ICDs.</i>
8	IT & NSS	If the capability will interface with or use JWICS or other intelligence managed dissemination means to receive or transmit information, ensure bandwidth requirements & quality of service requirements are addressed. (These will be a rough order of magnitude for CDDs.)

Table G-2. CDD and CPD Intelligence Considerations

**Para Para Title CDD and CPD Considerations, continued.**

9	Intel Support-ability	See the subparagraphs detailing paragraph 9 requirements below as well as Enclosure D of this instruction.
10	E3 & Spectrum Support	If there are potential issues regarding interference from threat emitters, ensure these issues are identified here and ensure consistency with the threat discussion in paragraph 4 or in the related threat references (must be DIA validated for ACAT ID). For clarity, include a pointer in this paragraph back to paragraph 4 or to the appropriate threat reference.
11	Assets Req'd for IOC	No additional requirements beyond reference b.
12	Schedule for IOC	Ensure the timeframe projected for any associated enabling future intelligence capabilities is consistent with the capability's projected IOC.
13	DOTMLPF Considerations	If any intelligence-related DOTMLPF considerations have been identified through related ISP processes or during analysis done for paragraph 9, ensure these are addressed here (or include a pointer to paragraph 9).
14	Other Attributes	If the capability is an ISR or ISR-related capability, ensure information protection standards are addressed.
15	Program affordability	No additional requirements beyond reference b.
App A	CRD Crosswalks	If any key intelligence CRDs or MA ICDs are referenced (DCGS, IG, MASINT/USMS, SIGINT, UCS/SIGINT), ensure KPPs support (not necessarily match) the KPPs identified in the CRD.
App B	Architecture Graphics	
OV-2	Ensure that intelligence systems are identified as specifically as possible considering program maturation, that applicable needlines are drawn, and that information attributes (as discussed in the DoDAF) for each exchange are included.	
OV-4	Ensure key intelligence contributing or receiving organizations are represented.	
OV-5	Ensure key intelligence activities are represented. Ensure the intelligence support requirements addressed in paragraph 9 are consistent with these activities.	
OV-6c	Ensure activity sequencing and timing for key intelligence support functions are addressed. Ensure a joint ISR context is represented, regardless of direct interfaces with intelligence nodes.	
SV-4	Ensure any specific systems tied to the intelligence information needs identified in the OV-2 are represented.	
SV-5	Ensure key intel activities from the OV-5 are represented in the SV-5 matrix.	
SV-6	Ensure specific exchange and data details for intelligence information (from systems) are addressed. Be as specific as possible with regard to content, format, accuracy, units of measurement, periodicity, timeliness, and security WRT Enclosure E guidelines for intelligence information. If "SCI" is listed as a security level, ensure security considerations per Director of Central Intelligence Directives (DCIDs) 6/3 and 6/9 are addressed within the text of the CDD/CPD.	
App C	Refs	Ensure threat references are current and DIA-validated as required, and that the appropriate intelligence CRDs or MA ICDs are listed.

Para	Para Title	ORD/ORD Annex/ORD Update Consideration
1	General Description of Operational Capability	<p>If the system possesses intelligence capabilities (such as signature collection, imaging, etc), ensure appropriate intel CRDs or MA ICDs have been listed if applicable (DCGS, IG, USMS, SIGINT, or UCS).</p> <p>If intelligence support is a key enabler of this system, ensure intelligence is addressed generally as a "support concept."</p> <p>Ensure the C4ISR (information exchange) concept been addressed.</p>
2	Threat	Ensure the threat to be countered has been summarized as well as the projected threat environment described. If the program is a Major Defense Acquisition Program, ensure DIA-validated threat assessments are cited. References must be current.
3	Shortcomings of Existing Systems and C4ISR Architectures	If there are known or projected shortfalls related to intelligence architecture, these must be generally addressed in this section. If the program is an intelligence provider, this will be related to paragraph 1 where the mission need is summarized.
4	Capabilities Required	If there are any threat-related factors that drive the timing needed for the capability in consideration, ensure those are addressed (refer back to paragraph 2 as appropriate). Ensure KPPs incorporate those factors as appropriate. Identify all intelligence capability KPPs that are vital to the system's primary mission. Ensure these KPPs support or exceed applicable intelligence CRDs or MA ICDs as detailed in paragraph 1 criteria above.
a	System Performance	Ensure threat has been adequately represented in mission scenarios. Ensure any intelligence-related support aspects of performance have been addressed as performance parameters (e.g. Target Location Error [TLE] if TLE is a critical variable in a weapon's overall accuracy).
b	Interoperability/ Net-Ready KPP	Ensure requirements for intelligence enabling information are addressed in the remaining Interoperability KPP elements or existing NR-KPP elements IAW CJCSI 6212.01C and JROCM 236-03 (19 Dec 03).
c	Logistics and Readiness	No additional requirements beyond reference o.
d	Env't, Safety, Operational Health	Ensure physical security requirements WRT TS/SCI policies have been addressed (such as DCID compliance as addressed in Enclosure D).
5	Program Support	General paragraph guidance: Ensure interfacing systems at the system/subsystem, platform, and force levels, specifically those related to intelligence, have been addressed.
a	Maintenance Planning	No additional requirements beyond reference o.
b	Support Equipment	No additional requirements beyond reference o.
c	C4I/ Standardization, Interoperability, and Commonality	<ul style="list-style-type: none"> <li>• Ensure subparagraph addresses how the system under review will be integrated into the intelligence architecture forecasted to exist at the time of operational fielding (e.g., Will it require new, materiel, intelligence capabilities? Are there dependencies on unprogrammed systems?)</li> <li>• Ensure the methodology for the above assessment is addressed. (5c guidance is continued on next page)</li> </ul>

Table G-3. ORD/ORD Annex/ORD Update Considerations

Para	Para Title	ORD/ORD Annex/ORD Update Consideration, contd.
c	C4I/ Standardization, Interoperability, and Commonality (contd)	<ul style="list-style-type: none"> <li>• Ensure unique intelligence information requirements (and associated dissemination or exchange requirements) are addressed here and in the OV-3 as appropriate. In this context, “unique” may apply to the nature, quantitative or qualitative attributes of the information, and should address intelligence information needs throughout the acquisition lifecycle. Enclosures D and E give examples of intelligence information requirements. Compliance and registration of intel data and metadata standards IAW references r and q.</li> <li>• With regard to information assurance, if the system is expected to interface with TS/SCI systems, ensure compliance with DCID 6/3 (reference m) is addressed.</li> </ul>
d	Computer Resources	If intelligence computer resource systems (e.g. USAF Raindrop terminals for coordinate mensuration) have not already been identified elsewhere, ensure they are addressed here.
e	Human Systems Integration	If applicable, ensure broad manpower constraints for intelligence support personnel are addressed. Ensure general skill requirements (such as language skills, training required) are addressed.
f	Other Logistics and Facilities Considerations	Ensure physical considerations (to include DCID 6/9 [reference n] compliance) for protection of TS/SCI material are addressed (if not already addressed in paragraph 4d).
g	Transportation and Basing	No additional requirements beyond reference o.
h	Geospatial Information and Services	If not already addressed in paragraph 5c, ensure requirements for geospatial information and services are addressed. Be as specific as possible.
i	Natural Env't Support	No additional requirements beyond reference o.
j	Env't and Health Impact	No additional requirements beyond reference o.
k	Safety	No additional requirements beyond reference o.
6	Force Structure	If the system under review is an intelligence provider or enabler, ensure the number of systems and subsystems estimated has been addressed.
7	Schedule	Operational Capability and projected Full Operational Capability increases, ensure the increase is considered and addressed in quantitative estimates.
8	Affordability	No additional requirements beyond reference o.
Appendixes		
A	References	Ensure the most current threat references (for ACAT ID, must be DIA-validated), appropriate DCIDs and CRDs or MA ICDs are properly cited.
B	Distro List	No additional requirements beyond reference o.
C	Supporting ORD Analysis	No additional requirements beyond reference o.
D	CRD Crosswalks	Ensure crosswalks with applicable, key intelligence CRDs are addressed (DCGS, IG, USMS, MTI, or UCS).

5. Developing Paragraph 9 of Capability Development Documents/ Capability Production Documents Intelligence Supportability. The intent of the Intelligence Supportability paragraph is not to duplicate intelligence support requirements already addressed in other sections of the document, but to ensure that all such requirements have been comprehensively addressed by either explicitly stating them in this section, or providing direct pointers to other sections within the document that already do. In some cases, basic requirements for intelligence support might be addressed, but the level of detail required to assess intelligence supportability (such as qualitative or quantitative attributes) is inadequate. In this instance, the drafter should elaborate to comply with reference b and facilitate a comprehensive intelligence supportability assessment IAW this instruction.

a. Level of Detail. The level of detail in this paragraph will usually increase as an acquisition program proceeds from the initial Milestone B CDD to the final Milestone C CPD of the last increment. The type of information required for this paragraph requires significant analysis of current and projected intelligence capabilities, manpower, resources and processes. In some instances, depending on the timeline of the program, intelligence capabilities may substantially mature in the interim, which will, in turn, change the next iteration of CDD or CPD documentation. The intelligence support requirements addressed in this paragraph will inherently be tied to the analysis of requirements and planned solutions as of the time of document drafting. The sponsor, however, is also responsible for identifying what requirements (and associated supportability) are unknown, or which cannot be reasonably assessed given what is known about the expected intelligence architecture. As discussed above, the sponsor should leverage the analysis and drafting efforts of the related ISP.

b. Scope. This paragraph (and the analysis behind it) should be based upon representative, validated scenarios and operational environments, and is not expected to address all possible contingencies. The paragraph must address *all* requirements for direct intelligence support to a capability, regardless of whether the type or nature of support to be provided is unique to the program.

c. Recommended Analytical Approaches. There are a number of analytical approaches that should be taken collectively to ensure a program's intelligence support requirements are adequately defined. These approaches include:



(1) Review the completed or ongoing analysis from the Information Needs Discovery and Analysis Process related to the program's associated ISP drafting efforts. Depending on the maturity and completeness of the ISP drafting efforts and associated analysis, some elements of the approaches below may already be accomplished.

(2) Review the associated architecture graphics for intelligence based on information needs. Determine whether the information needs in such graphics are covered in enough detail to assess supportability (as defined in Enclosure E). Likewise, if graphics appear incomplete based upon intelligence support identification efforts, ensure intelligence information needs are reflected.

(3) Carefully examine operational performance requirements in CDD and CPD paragraph 6 (System Capabilities Required for the Current Increment). What intelligence information is required to support those capabilities? For those information requirements identified, what intelligence infrastructure (e.g., platforms, systems, software, facilities) and resources (e.g., manpower, funding) are required to directly generate and deliver the information required? (Note: The sponsor is not expected to "reverse analyze" the entire intelligence cycle back to the source collection.) For the information requirements identified, are those captured within the appropriate architecture graphics (and if so, do they have sufficient detail to assess supportability)?

(4) Analyze the capability's projected progression throughout the acquisition life cycle and identify intelligence requirements to the "pre-operational" phases such as development, testing and training.

d. Recommended Format. Paragraph organization is flexible and may be tailored to best fit the style of the document, but the following provides a recommended format:

9. Intelligence Supportability. Introduce paragraph with a general description of the level of intelligence support required to enable the program's warfighting capability. For all requirements below, be as specific as possible, and include as many qualitative and quantitative attributes as possible (e.g., accuracy, timeliness, estimated volume, required update rates). If detail regarding required qualitative or quantitative attributes is unknown due to program maturity (such as awaiting source selection), state what is not known and why. If requirements are discussed in other places within the document already, provide pointers to those paragraphs.

9a. Intelligence Support to Development. This should, as a minimum, reference intelligence threat support and refer back to paragraph 4 as appropriate.

9b. Intelligence Support to Development and Testing. Using the “System Development and Demonstration” column under the “Acquisition Cycle Applicability” header in Enclosure D as a guide, address required intelligence support to program testing. Ensure intelligence information or services required to ensure a capability can be tested in its intended environment.

9c. Intelligence Support to Training. Address whether intelligence support is required to contribute to any training programs associated with operation or implementation of the capability.

9d. Intelligence Support to Operations. Using the “Operations and Support” column under the “Acquisition Cycle Applicability” header in Enclosure D and Enclosure E as guides, address requirements for intelligence support to ensure successful operation of the capability.

9e. Intelligence Security Requirements. Demonstrate that security considerations such as classification levels, releasability and physical facility implications for Sensitive Compartmented Information have been addressed (e.g., compliance with references m and n).

9f. Potential Intelligence Support Shortfalls. Address known, projected or potential shortfalls in required intelligence support capabilities, to include manpower, training, doctrine, processes or systems that could degrade the operational effectiveness of the system, or impede its development, testing or training. Address the assessed cause of these shortfalls, such as technological capability shortfalls, undefined common intelligence data/metadata standards, scheduling disconnects (dependencies on projected intelligence capabilities not yet fielded by system Initial Operating Capability), or funding issues. (Note: In many cases, intelligence shortfalls may be classified; ensure that proper security guidelines are followed.) Estimate the impact of failure to resolve the shortfalls in terms of program resources and schedule, inability to achieve threshold performance, and/or system or warfighter vulnerability.

9g. Proposed Solutions. If solutions to identified shortfalls fall within the scope of the program office, identify the plan and schedule to remedy each shortfall, including key issues that must be resolved. If the solution lies outside the control of the program office, provide a recommendation identifying the organization with the responsibility and authority to address the shortfall.

6. Information Support Plan Document Development. Reference h defines an information need as a condition or situation requiring knowledge or intelligence derived from, received, stored or processed facts and data. The ISP process is meant to help identify and resolve

implementation issues related to both information infrastructure support and information interface requirements. The table below will identify specific areas within the ISP, by paragraph, the program manager should consider with respect to the intelligence certification.

Ch	Title	ISP Consideration
1	Intro- duction	<p>a. Overview. Address how the capability relates to the BA integrated architecture, or other intel support elements of other JFAs/JFCs (like targeting sub-architectures as part of the Force Application JFA/JFC). Address whether the desired capabilities described relate to any of the key intelligence CRDs or MA ICDs.</p> <p>b. Program Data. Address any program related acquisition scheduling issues that have precluded conducting full intelligence information need and supportability analysis. For example, system level detail may not be available until prime contractor selections have been made, or until the functional solution has been more refined.</p>
2	Analysis <i>(Steps correspond with steps in the Information Needs and Discovery Process described in reference h)</i>	<ul style="list-style-type: none"> <li>• Ensure the warfighting missions or enterprise business domain functions are consistent with the operational capabilities required IAW the associated CDD or CPD. (Step 1)</li> <li>• Ensure intelligence information needs are completely addressed, clearly related to the missions or functions identified in Step 1 and include required qualitative and quantitative attributes as discussed in Enclosure E of this instruction. (Steps 2, 4, 5 and 6)</li> <li>• Ensure the scope of analysis for and declaration of intelligence information needs includes all stages of acquisition (to include development, testing, training, and operation). (Step 13)</li> <li>• Ensure the supportability assessment adequately considers the ability of the current/projected joint intelligence architecture to both quantitatively and qualitatively satisfy the intelligence information needs. (Step 8)</li> <li>• Ensure the analysis in this section is consistent with intelligence information needs discussed in the associated CDD or CPD (primarily paragraph 9).</li> </ul>
3	Issues	Ensure intelligence related shortfalls, issues, and associated mitigation strategies or resolution paths have been addressed. Ensure this section is consistent with paragraph 9 of the associated CDD or CPD.
App A	Refs	Ensure the Battlespace Awareness Joint Functional Concept is cited if applicable. Ensure the currency of any relevant DIA or Service-validated threat references used.
App B	SV-6	Ensure intelligence nodes and systems/subsystems have been adequately represented in the Systems Information Exchange Matrix (SV-6). Ensure specific exchange and data details for intelligence information (from systems) are addressed. Be as specific as possible with regard to content, format, accuracy, units of measurement, periodicity, timeliness, and security WRT Enclosure E guidelines for intelligence information. If "SCI" is listed as a security level, ensure security considerations per Director of Central Intelligence Directives (DCIDs) 6/3 and 6/9 are addressed within the text of the CDD/CPD.
App C	N/A	N/A (Interface Control Agreements)
App D	Acronyms	Ensure appropriate intelligence-related acronyms are included for clarity.

Table G-4. ISP Intelligence Considerations

(INTENTIONALLY BLANK)

ENCLOSURE H

REFERENCES

- a. CJCSI 3170.01 Series, "Joint Capabilities Integration and Development System."
- b. CJCSM 3170.01 Series, "Operation of the Joint Capabilities Integration and Development System."
- c. CJCSI 5123.01 Series, "Charter of the Joint Requirements Oversight Council."
- d. CJCSI 6212.01 Series, "Interoperability and Supportability of National Security Systems and Information Technology Systems."
- e. DODD 5000.1, 12 May 2003, "The Defense Acquisition System."
- f. DODI 5000.2, 12 May 2003, "Operation of the Defense Acquisition System."
- g. DODD 4630.5, 5 May 2004, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)."
- h. DODI 4630.8, 30 June 2004, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)."
- i. DODD 5105.21, 18 February 1997, "Defense Intelligence Agency."
- j. DIA Regulation 55-3, 15 May 1998, "Intelligence Support for Defense Acquisition Programs."
- k. Acquisition Knowledge Sharing System (AKSS), "Acquisition Deskbook," <http://asks.dau.mil/jsp/default/jsp>.
- l. DODD 8500.1, 24 October 2002, "Information Assurance."
- m. Director of Central Intelligence Directive (DCID) 6/3, 5 June 1999, "Protecting Sensitive Compartmented Information within Information Systems."
- n. DCID 6/9, 18 November 2002, "Physical Security Standards for Sensitive Compartmented Information Facilities."

- o. CJCSI 3170.01 Series, "Requirements Generation System."
- p. CJCSM 3500.04 Series, "Universal Joint Task List."
- q. Interim Defense Acquisition Guidebook (formerly DOD Regulation 5000.2-R, 5 April 2002), 30 October 2002.
- r. Intelligence Community Policy for Metadata and Metadata Markup, 15 April 2003, Intelligence Community Chief Information Officer Executive Council.
- s. DOD Architecture Framework Version 1.0, Volume II, Product Descriptions, 9 February 2004.
- t. CJCS 3137 Series, "The Functional Capabilities Board Process."
- u. JROCM 095-04, 14 June 2004, "Capstone Requirements Documents (CRDs) Conversion Guidance."
- v. DODD 5200.39, 10 September 1997, "Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection."
- w. JROCM 124-04, 9 July 2004, "Common Data Standards and Format to Enable Horizontal Integration (HI)."
- x. DCID 1/8, 21 March 2001, "Management of National Imagery, Imagery Intelligence, Geospatial Activities, and Related Information."
- y. DODD 5105.60, 11 October 1996, "National Imagery and Mapping Agency."
- z. DODD 5200.37, 18 December 1992, "Centralized Management of Department of Defense Human Intelligence (HUMINT) Operations."
- aa. DODD 5100.20, 23 December 1971 (Administrative Reissuance Incorporating Through Change 4, June 24, 1991), "The National Security Agency and the Central Security Service."
- bb. JSM 5100.01 Series, "Organization of the Joint Staff."

## GLOSSARY

### PART I--ABBREVIATIONS AND ACRONYMS

ACAT	Acquisition Category
BA	Battlespace Awareness
BA FCB	Battlespace Awareness Functional Capability Board
BAWG	Battlespace Awareness (FCB) Working Group
BDA	Battle Damage Assessment
C2	command and control
C4	command, control, communications and computers
C4I	command, control, communications, computers and intelligence
C4ISP	command, control, communications and intelligence support plan
CDD	Capability Development Document
CIC	critical intelligence category
CIO	Chief Information Officer
CPI	critical program information
CPD	Capability Production Document
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CONOPS	concept of operations
CRD	Capstone Requirements Document
CSAR	combat search and rescue
CSS	Central Security Service
DAB	Defense Acquisition Board
DCID	Director, Central Intelligence Directive
DCGS	Distributed Common Ground/Surface System
DIA	Defense Intelligence Agency
DIA/DR	Director, Defense Intelligence Agency
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODIIS	Department of Defense Intelligence Information System
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel and facilities
FAA	Functional Area Analysis
FNA	Functional Needs Analysis
FSA	Functional Solutions Analysis
FCB	Functional Capabilities Board

GDIP	General Defense Intelligence Program
HUMINT	human intelligence
IA	information assurance
IC	Intelligence Community
ICD	initial capabilities document
ICMR	Intelligence Community Metadata Registry
ICWG	intelligence certification working group
IMINT	imagery intelligence
INFOSEC	information security
IPB	intelligence preparation of the battlespace
IRCO	Intelligence Requirements Certification Office
ISP	Information Support Plan
ISR	intelligence, surveillance and reconnaissance
IT	information technology
ITWA	Initial Threat Warning Assessment
JCIDS	Joint Capabilities Integration and Development System
JCPAT-E	Joint C4I Program Assessment Tool-Empowered
JCS	Joint Chiefs of Staff
JiIB	Joint Intelligence Interoperability Board
JIPB	Joint Intelligence Preparation of the Battlespace
JITC	Joint Interoperability Test Command
JMIP	Joint Military Intelligence Program
JPD	Joint Potential Designator
JROC	Joint Requirements Oversight Council
JSBA	Joint Systems Baseline Assessment
JWICS	Joint Worldwide Intelligence Communications System
KM/DS	Knowledge Management/Decision Support tool
MA ICD	Mission Area Initial Capabilities Document
MASINT	Measurement and Signatures Intelligence
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MEA	Munitions Effects Assessment
MER	Manpower Estimation Report
METOC	meteorological and oceanographic
MNS	Mission Need Statement
MTI	Moving Target Indicator
NFIP	National Foreign Intelligence Program
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
NSP/SMO	National Signatures Program Systems Management Office



NSA/CSS NSS	National Security Agency/Central Security Service national security systems
OPSEC	operational security
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
POC	point of contact
SIGINT	signals intelligence
SIPRNET	Secret Internet Protocol Router Network
TECHINT	technical intelligence
TIARA	Tactical Intelligence and Related Activities
TLE	target location error
TTPs	tactics, techniques and procedures
UCS	Unified Cryptologic System
USMS	US MASINT System
XML	Extensible Markup Language

## PART II--DEFINITIONS

Acquisition Category (ACAT). Categories established to facilitate decentralized decision-making and execution, and compliance with statutorily imposed requirements. The categories determine the level of review, decision authority and applicable procedures. Reference f provides the specific definition for each acquisition category (ACAT I through III).

availability. In the context of this CJCSI, an assessment that the intelligence information, infrastructure or resources are, or are expected to be, available to support the operational system or program throughout all phases of its life cycle. This assessment takes into consideration the operational requirements and acquisition schedule of the system or program, current and proposed defense and national intelligence support infrastructures, C4I architectures, funding levels and allocations and other materiel and non-materiel issues.

command, control, computers, communication and intelligence support plan (C4ISP). The C4ISP was the document formerly required by the DOD 5000 and 4630 Series; it has since been replaced by the Information Support Plan. The purpose of the C4ISP was to provide a window into a specific system development program through which can be seen C4ISR needs, dependencies, interfaces and any shortfalls in the C4I required for each phase of the system's life cycle.

Capability Development Document (CDD). A document that captures the information necessary to develop a proposed program(s), normally using an evolutionary acquisition strategy. The CDD outlines an affordable increment of militarily useful, logistically supportable and technically mature capability.

Capability Production Document (CPD). A document that addresses the production elements specific to a single increment of an acquisition program.

Capstone Requirements Document (CRD). A document that contains capabilities-based requirements that facilitates the development of CDDs and CPDs by providing a common framework and operational concept to guide their development.

certification. A statement of adequacy provided by a responsible agency for a specific area of concern in support of the validation process.

DOD component. The DOD components consist of the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Defense agencies, DOD field activities and all other organizational entities within the Department of Defense.

Functional Capability Board. A permanently established body that is responsible for the organization, analysis and prioritization of joint warfighting capabilities within an assigned functional area.

Gatekeeper. That individual who makes the initial joint potential designation of JCIDS proposals. This individual will also make a determination of the lead and supporting FCBs for capability proposals. The Gatekeeper is supported in these functions by USJFCOM, J-6, J-7 and the FCB Working Group leads. The Vice Director, J-8 serves as the Gatekeeper.

geospatial intelligence. The term “geospatial intelligence” means the exploitation and analysis of imagery and geospatial information to describe, assess and visually depict physical features and geographically referenced activities on the earth. Geospatial intelligence consists of imagery, imagery intelligence and geospatial information.

information technology (IT). Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services) and related resources. Information technology does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Initial Capabilities Document. Documents the need for a materiel approach to a specific capability gap derived from an initial analysis of materiel approaches executed by the operational user and, as required, an independent analysis of materiel alternatives. It defines the capability gap in terms of the functional area, the relevant range of military operations, desired effects and time. The ICD summarizes the results of the DOTMLPF analysis and describes why nonmaterial changes alone have been judged inadequate in fully providing the capability. (Also see Mission Area ICD.)

Information Support Plan (ISP). The ISP provides a mechanism to identify and resolve implementation issues related to an acquisition program's information technology (IT) and National Security Systems information infrastructure support and information interface requirements. It identifies IT and information (including intelligence) needs, dependencies and interfaces for programs in all acquisition categories, focusing on net-readiness, interoperability, information supportability and information sufficiency concerns.

intelligence certification. The affirmation that requirements for intelligence support have been completely and adequately declared and identified; adequately assessed for projected supportability; that critical intelligence supportability or threat-related issues identified during coordination of program documents have been addressed; and that any projected shortcomings in intelligence support will be dealt with in an appropriate manner. This certification occurs as a prerequisite for the Joint Capabilities Integration and Development System (JCIDS) and defense acquisition processes and occurs at each acquisition milestone.

intelligence requirements. For the purposes of this CJCSI, intelligence requirements refer to requirements for intelligence information, infrastructure or systems (as opposed to intelligence collection requirements).

intelligence supportability. The availability, suitability and sufficiency of intelligence information and capabilities to support the requirements or system defined in program documents.

interoperability. (1) The ability of systems, units or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together and (2) The condition achieved among communications, electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them or their users.

interoperability certification. A J-6 certification process that parallels the intelligence certification process in which DIA and J-2 are assessor and contributing organizations. (See reference d for further details.)

Joint C4I Program Assessment Tool-Empowered (JCPAT-E). A tool set that DISA operates and maintains for the Joint Staff and OASD(NII) that provides a collaborative work area, automated mail and distribution function and an archival capability.

Joint Potential Designator. A designation assigned by the Gatekeeper to specify JCIDS validation, approval and interoperability expectations.

a. “JROC Interest” designation will apply to all ACAT I/IA programs and programs designated as JROC Interest. This designation may also apply to intelligence capabilities that support DOD and national intelligence requirements. These documents will be staffed through the JROC for validation and approval. All CRDs (or MA ICDs) will be designated as JROC Interest. DOTMLPF change proposals will also be designated as JROC Interest in accordance with reference c.

b. “Joint Integration” designation will apply to ACAT II and below programs where the concepts and/or systems associated with the document do not significantly affect the joint force and an expanded review is not required, but National Security Systems and Information Technology Systems (NSS and ITS) interoperability, intelligence or munitions certification is required. Once the required certification(s) are completed, Joint Integration proposals are validated and approved by the sponsoring Component.

c. “Independent” designation will apply to ACAT II and below programs where the concepts and/or systems associated with the document do not significantly affect the joint force, an expanded review is not required, and no certifications are required. Once designated, these documents are returned to the sponsoring component for validation and approval.

Knowledge Management/Decision Support tool (KM/DS). A tool set that replaced the legacy system JCPAT for processing, coordination and document repository functions for JCIDS documents. KM/DS will facilitate staffing and commenting functions for JROC Interest and Joint Impact documents.

Mission Area Initial Capabilities Documents (MA ICDs). MA ICDs were created by the JROC via JROCM 095-04 and are permanently replacing Capstone Requirements Documents. MA ICDs are considered the next step in ensuring that capabilities contribute to specific mission areas and comply with the standards and Key Performance Parameters necessary for specific accomplishment of that mission.

national security systems (NSS). Telecommunications and information systems operated by the Department of Defense--the functions, operation or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves the command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons systems; or (5) is critical to the

direct fulfillment of military or intelligence missions. Subsection (5) in the preceding sentence does not include procurement of automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance, logistics and personnel management applications).

Net-ready. DOD IT/NSS that meets required information needs, information timeliness requirements, has information assurance accreditation, and meets the attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. DOD IT/NSS that is Net-ready enables warfighters and DOD business operators to exercise control over enterprise information and services through a loosely coupled, distributed infrastructure that leverages service modularity, multimedia connectivity, metadata and collaboration to provide an environment that promotes unifying actions among all participants. See reference d for more information.

sufficiency. In the context of this CJCSI, an assessment whether the intelligence information, infrastructure and/or resources are, or are expected to be, sufficient to support the operational capability, system or program. This assessment takes into consideration the operational requirements and acquisition schedule of the system or program and determines the minimum requirements for the current and proposed defense and national intelligence support infrastructures, C4I architectures, funding levels and allocations, and other materiel and non-materiel activities.

suitability. In the context of this CJCSI, an assessment whether the intelligence information, infrastructure and/or resources are, or are expected to be, suitable to support the operational system or program. This assessment takes into consideration the operational requirements and acquisition schedule of the system or program and determines if the current or proposed defense and national intelligence support infrastructures, C4I architectures, and funding levels and allocations are, or are expected to be, what is required to satisfy the operational need.